ДО
ЕСО ЕАД
гр. София 1618
бул. „Цар Борис III“ № 201

ПРЕДЛОЖЕНИЕ
за изпълнение на обществена поръчка с предмет:
„Доставка на телемеханични системи“

От АББ България ЕООД

Представяме Ви нашето предложение за изпълнение на обществената поръчка по обявената процедура с горепосочения предмет, както следва:

1. Предлагаме срок за изпълнение на първоначалната доставка 140 календарни дни от датата на изпращане на поръчка за доставка (включително приемни изпитания, обучение в учебен център, конфигуриране и въвеждане в експлоатация на RTU в п/ст Елин Пелин, п/ст Бабово и п/ст Капитан Петко).

** Срокът за изпълнение на първоначалната доставка е не повече от 140 календарни дни от датата на изпращане на поръчка за доставка.*

2. Предлагаме срок за доставка по всяка отделна поръчка за доставка: 84 календарни дни от датата на изпращане на конкретна поръчка за доставка.

***Срокът за изпълнение на доставка по всяка отделна поръчка за доставка е не повече от 84 календарни дни от датата на изпращане на конкретна поръчка за доставка.*

3. Предлагаме гаранционнен срок за доставената апаратура: 42 месеца датата на подписан протокол за съответната доставка.

**** Гаранционният срок за доставената апаратура е не по-малко от 42 месеца от датата на подписан протокол за съответната доставка.*

4. Като неразделна част от настоящото приложение за изпълнение на поръчката прилагаме следните документи (*Допустимо е приложенията към техническо приложение да бъдат представени на български или на английски език*):

4.1. Декларация за съответствие (declaration of comformity), изготвена съгласно изискванията на **БДС EN.ISO/IEC 17050-1 и 17050-2.**

4.2. Попълнена **Таблица А** „Обем на първоначална доставка до склад на възложителя", към т. А.2 от раздел I от документацията за участие, като се спазват указанията към тази таблица.

4.3. Попълнена **Таблица В** „Предложение на участника за конфигурация на RTU" към т. А.2 от раздел I от документацията за участие, като се спазват указанията към тази таблица.

4.4. Попълнена **Таблица Г** „Съответствията на RTU с минималните изисквания на Възложителя" към т. А.2 от раздел I от докуметцията за участие, като се спазват указанията към тази таблица.

4.5. Таблица в **Приложение 1** от раздел I от докуметацията за участие – предложение, отговарящо на „Минималните изисквания към всяка конфигурация".

4.6. Описание на работа по протокол IEC 60870-5-101 (interoperability sheet), съответстваща на изискванията, описани в и на описаната в **Приложение 3**

4.7. Описание на работа по протокол IEC 60870-5-104 (interoperability sheet), съответстваща на изискванията, описани в **Приложение 4**

4.8. Описание на работа по протокол IEC 60870-5-103 (interoperability sheet), съответстваща на изискванията, описани в **Приложение 5**

4.9. Описание на работа по протокол Modbus/RTU (interoperability sheet), съответстваща на изискванията, описани в **Приложение 6**

4.10. Таблица в **Приложение 7** от раздел I от докуметацията за участие – Изисквания по стандарт за сигурност IEC 62351.

4.11. Таблици 1, 2 и 3 в **Приложение 9** от раздел I от докуметацията за участие - Изисквания към работата на RTU по стандарт IEC61850

4.12. Декларации от типа ACSI (Abstract Communication Service Interface), PICS (Protocol Implementation Conformance Statement), PIXIT (Protocol Implementation eXtra Information for Testing), MICS (Model Implementation Conformance Statement), TICS (Tissues Conformance Statement), Interoperability sheet, както е приложимо за поддържаните от RTU протоколи за комуникация.

4.13. Сертификати, издадени от акредитирани лица, удостоверяващи съответствието на телемеханичните системи от предлаганата серия със стандарти от сериите БДС EN 61850 Ed1, БДС EN 61850 Ed2, БДС EN 60870, БДС EN 62351-3 или техни еквиваленти

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

4.14. Схеми на цифрови входове, цифрови изходи, аналогови входове, аналогови изходи.

4.15. Параметри на комуникационния канал за дистанционно конфигуриране и тестване на RTU от работните станции и минималните изисквания за сигурност към този комуникационния канал.

4.16. Изчислената по дадената в **Приложение 8** от раздел I от докуметацията за участие методика разполагаемост на всяка от предложените конфигурации.

4.17. Описание на фирмената политика на Производителя за жизнения цикъл на предлаганите изделия и на частите за тяхната поддръжка.

4.18. Описание на техническите характеристики на предлаганите от участника изделия. Представят се документи съдържащи техническа спецификация, като каталози, проспекти или технически данни на изделието.

5. Декларираме, че:

5.1. Телемеханичните системи, които предлагаме ще са произведени от АББ АГ.

5.2. Приемаме клаузите на приложения в документацията за участие в процедурата проект на проект на договор.

5.3. Направените от нас предложения и поети ангажименти са валидни за срока, посочен в обявлението, считано от датата на подаване на офертата.

Гарантираме, че сме в състояние да изпълним качествено поръчката в пълно съответствие с изискванията на възложителя.

Приложения:

1. Декларация за конфиденциалност по чл. 102 от ЗОП (когато е приложимо)
2. Документ за упълномощаване, когато лицето, което подава офертата, не е законният представител на участника (когато е приложимо).

Дата: 11.04.2019 г.

Заличено по чл. 36а, ал.3 от ЗОП

ПОДПИС и ПЕЧАТ:

Марсел Заличено по чл. 36а, ал.3 от ЗОП Хук
Управител
АББ България ЕООД

Стефан Минчев
Управител
АББ България ЕООД

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

Документ 4.1.

Декларация за съответствие (declaration of comformity), изготвена съгласно изискванията на БДС EN.ISO/IEC 17050-1 и 17050-2.

Konformitätserklärung
Declaration of Conformity

ABB AG

Wir (Name des Anbieters) _____
We (supplier's name)

Kallstadter Straße 1
68309 Mannheim

Anschrift _____
Address

Diese Konformitätserklärung entspricht der Europäischen Norm EN 45014 "Allgemeine Kriterien für Konformitätserklärungen von Anbietern". Die Grundlage der Kriterien sind internationale Dokumente, insbesondere ISO/IEC-Leitfaden 22, 1982, "Informations on manufacturer's declaration of conformity with standards or other technical specifications".

This Declaration of Conformity is suitable to the European Standard EN 45014 "General criteria for supplier's declaration of conformity". The basis for the criteria has been found in international documentation, particularly in: ISO/IEC Guide 22, 1982, "Informations on manufacturer's declaration of conformity with standards or other technical specifications".

erklären in alleiniger Verantwortung, daß das Produkt
declare under our sole responsibility that the product

Fernwirk-Unterstation
Remote Terminal Unit

ABB RTU 560

(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Serien-Nr., möglichst Herkunft und Stückzahl)
(name, type or model, batch or serial number, possibly sources and number of items)

auf das sich diese Erklärung bezieht, mit der/den folgenden Norm(en) oder normativen Dokument(en) übereinstimmt.
to which this declaration relates is in conformity with the following standard(s) or other normative document(s).

EN 61000-6-2: 2006-03 + Ber 1:2011-06
EN 61000-6-4: 2007 + A1:2011
EN 60950-1: 2006-A11:2009/A1:2010/A12:2011/A2:2013

(Titel und/oder Nr. sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente/
Title and/or number and data of issue of the standard(s) or other normative document(s))

Gemäß den Bestimmungen der Richtlinie(n) (falls zutreffend)
Following the provisions of Directive(s) (if applicable)

EMV – Richtlinie Nr. 2014/30/EG
EMC Directive No. 2014/30/EC
Niederspannungsrichtlinie Nr. 2014/35/EG
Low Voltage Directive No. 2014/35/EC

Заличено по чл. 36а, ал.3 от ЗОП

PGGA-PP Sigbert Reimann

Заличено по чл. 36а, ал.3 от ЗОП

CE-Kennzeichnung in: 2009
CE marking in: 2009

Erklärung Nr.:
Declaration No.:
1 KGT 100 468 V 0011

Mannheim, 25.06.2016
(Ort und Datum der Ausstellung/
Place and date of issue)

PGGA-P Helmut Weber
(Name und Unterschrift oder gleichwertige Kennzeichnung des Befugten/
name and signature or equivalent marking of authorized person)

Anhang/Attachment:

Typ/type	Name/name	Identnummer/number
CMU Module/ modules	560CMU02	1KGT013100R0001
	560CMU05	1KGT012700R0002
	560CMR01	1KGT036200R0001
	560CMR02	1KGT036300R0001
	560HMR01	1KGT030500R0001/2
Netzteil/ power supply	560PSR00	1KGT026500R0001
	560PSU01	1KGT006600R0002
	560PSU02	1KGT011900R0001
E/A Module/ IO modules	560BIR01	1KGT034000R0001/2
	23BE23	1KGT012100R5001
	560BOR01	1KGT036800R0002
	23BA20	GSNE000700R5312
	23BA23	1KGT020800R0001
	560AIR01	1KGT036500R0001
	560AIR02	1KGT037500R0001
	23AE23	1KGT012200R5001
	23AA21	1KGT020700R0001
	23BE50	1KGT020900R0001
	23BA40	1KGT011200R0011
	23BE40	1KGT011100R0011/12
Etage/ racks	560MPR01	1KGT012500R0001
	560BCU02	1KGT007900R0001
	560MPR03	1KGT022100R0001
	560BCU04	1KGT022300R0001/2/3
	560SFR02	1KGT022200R0001
	560BCU05	1KGT022400R0001/2/3
	560FPR01	1KGT007700R1002
Kommunikation/ communication	23OK24	1KGT011800R5001
	23WT23	1KGT008200R0001/2
	23WT24	1KGT010500R0001
	23WT25	1KGT012400R0001/2
	560NUS04	1KHW001891R0001
	560NUS12	1KHW001892R0001
	560NMS24	1KHW002108R0001
	560NMS34	1KHW023538R0001
Echtzeituhr/ Realtime clocks	560RTC01	1KGT006700R0001
	23AN02	1KGT006800R0001
	560RTC02	1KGT007800R0001
	25AN01	GSNP812601R0003
	560RTC03	1KGT012000R0001

Документ 4.2.

Попълнена Таблица А „Обем на първоначална доставка до склад на възложителя“, към т. А.2 от раздел I от документацията за участие, като се спазват указанията към тази таблица

Таблица А. Обем на първоначална доставка до склад на ВЪЗЛОЖИТЕЛЯ

№	Апаратура	Количество	Тип
I.	**RTU**	**21 бр**	Модел RTU
1	Комуникационен сървър за система за управление на подстанции (SAS комуникационен сървър)	20	RTU 560
2	Малък	1	RTU 560
3	Голям	0	RTU 560
II.	**Системи за конфигуриране, тестване и зареждане на RTU**	**Количество**	Наименование на SW
1.	Работни станции за конфигуриране на RTU	**2 бр.**	
2.	Лицензи за стандартен софтуер инсталирани на работните станции (по типове – операционна система, офис пакет и други, необходими за работа на компютърната конфигурация и на специализирания софтуер)	2 комплекта	Операционна система: **WinPro 10 SNGL OLP NL Legalization GetGenuine** Офис пакет: **OfficeStd 2019 SNGL OLP NL**
3.	Лицензи за специализирани софтуери инсталирани на работните станции, включваща минимум следното: - Лиценз за софтуер за конфигуриране и тестване на RTU - Лиценз за софтуер за конфигуриране на логически функции и аритметични изчисления	2 комплекта	Лиценз за софтуер за конфигуриране и тестване на RTU: **RTUtil500** Лиценз за софтуер за конфигуриране на логически функции и

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

			аритметични изчисления **MULTIPROG 5**
III.	**Специализирани софтуери за конфигуриране, тестване и зареждане на RTU**	**Количество**	Наименование на SW
1.	Лицензен специализиран софтуер, инсталационни пакети, включващи софтуера в т.II.3, който ще се инсталира от специалисти на Възложителя на компютърни конфигурации на Възложителя. - Лиценз за софтуер за конфигуриране и тестване на RTU - Лиценз за софтуер за конфигуриране на логически функции и аритметични изчисления	15 комплекта	Лиценз за софтуер за конфигуриране и тестване на RTU: **RTUtil500** Лиценз за софтуер за конфигуриране на логически функции и аритметични изчисления **MULTIPROG 5**
IV.	**Специализирани инструменти и приспособления**	**Количество**	Тип
1.	Специализирани инструменти и приспособления (ако е приложимо, да се опишат подробно в предложенията): - Инструмент за кримпване на процесни конектори - Инструмент за демонтаж на snap-in контакти - Инструмент за демонтаж на процесни конектори	5 комплекта	Инструмент за кримпване на процесни конектори: **Crimp tool for 23XS40 R4001** Инструмент за демонтаж на snap-in контакти

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

			Removal tool for snap-in contacts Инструмент за демонтаж на процесни конектори **Removal tool for process connector 23XS40 R3001**

Указания за попълване на позициите на бял фон в Таблица А:

Число – изискван минимален брой.

Многоточие („.....“) – Участниците да попълнят необходимата информация, където и за колкото реда е приложимо (при необлходимост се допълват редове, колкото е нужно за да се опише предложението на съответния Участник)

Непопълнено – Участниците да попълнят необходимата информация. Да не се оставят празни позиции.

АББ България ЕООД
Централен офис
бул. „Витоша“ № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

Документ 4.3.

Попълнена Таблица В „Предложение на участника за конфигурация на RTU“ към т. А.2 от раздел I от документацията за участие, като се спазват указанията към тази таблица

Таблица В. Предложение на участника за конфигурация на RTU

№	КОНФИГУРАЦИЯ НА RTU	ТИП RTU / МОДУЛ	БРОЙ
1.	**"Голям"**		
1.1.	Шкаф	ЕЛ -ТЕСТ -2200/800/800	1
1.2.1.	Шаси	560SFR02 R0001	1
1.2.1.1.	Общ брой слотове	Вградени в шасито	21
1.2.2.	Шаси	560SFR02 R0001	1
1.2.2.1.	Общ брой слотове	Вградени в шасито	21
1.2.3.	Шаси	560SFR02 R0001	1
1.2.3.1.	Общ брой слотове	Вградени в шасито	21
1.3.1.	Модули:		
1.3.1.1.	захранващ модул	560PSR00 R0001	2
1.3.1.2.	процесорен модул	560CMR02 R0001	2
1.3.1.3.	комуникационен модул	Вграден в процесорния модул	2
1.3.1.4.	модул аналогови входове	560AIR01 R0001	10
1.3.1.5.	модул цифрови изходи-сигнали	560BOR01 R0002	1
1.3.1.6.	модул входове цифрово измерване (BCD code – двоично-десетичен код)	560BIR01 R0001	1
1.3.2.	Модули:		
1.3.2.1.	захранващ модул	560PSR00 R0001	2
1.3.2.2.	модул цифрови входове	560BIR01 R0001	16

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

1.3.3.	Модули:		
1.3.3.1.	захранващ модул	560PSR00 R0001	2
1.3.3.2.	модул цифрови входове	560BIR01 R0001	7
1.3.3.4.	модул цифрови изходи-команди	560BOR01 R0002	2
1.3.3.5.	модул аналогови изходи	23AA21 R0001	2
1.4	Интерфейсни кабели за входни-изходните модули до репартитор (15 метра всеки)	TCBB 10x2x0,5	50
1.5	Други		
1.5.1	Модул цифрови входни Броячни сигнали	560BIR01 R0001	1
1.5.2	Връзка за процесна шина	560BCU05 R0001	1
1.5.3	Захранващ модул	CP-E 24/2.5	3
1.5.4	Лиценз	PLC/Archives License, SD-card	2
1.5.5	Клеми – 18 пина	23XS40 R3001	47
1.5.6	Кабелни накрайници	23XS40 R4001	846

№	КОНФИГУРАЦИЯ НА RTU	ТИП RTU / МОДУЛ	БРОЙ
2.	**„Малък“**		
2.1.	Шкаф	ЕЛ -ТЕСТ -2200/800/800	1
2.2.1	Шаси	560SFR02 R0001	1
2.2.1.1.	Общ брой слотове	Вградени в шасито	21
2.2.2	Шаси	560SFR02 R0001	1

2.2.2.1.	Общ брой слотове	Вградени в шасито	21
2.3.1	Модули:		
2.3.1.1.	захранващ модул	560PSR00 R0001	2
2.3.1.2.	процесорен модул	560CMR02 R0001	2
2.3.1.3.	комуникационен модул	Вграден в процесорния модул	2
2.3.1.4.	модул цифрови входове	560BIR01 R0001	12
2.3.2	Модули:		
2.3.2.1.	захранващ модул	560PSR00 R0001	2
2.3.2.2.	модул цифрови входове	560BIR01 R0001	3
2.3.2.3.	модул аналогови входове	560AIR01 R0001	5
2.3.2.4.	модул цифрови изходи-сигнали	560BOR01 R0002	1
2.3.2.5.	модул цифрови изходи-команди	560BOR01 R0002	2
2.3.2.6.	модул аналогови изходи	23AA21 R0001	2
2.3.2.7.	модул входове цифрово измерване (BCD code)	560BIR01 R0001	1
2.4	Интерфейсни кабели за входни-изходните модули до репартитор (15 метра всеки)	TCBB 10x2x0,5	21
2.5	Други		
2.5.1	Модул цифрови входни Броячни сигнали	560BIR01 R0001	1
2.5.2	Връзка за процесна шина	560BCU05 R0001	1
2.5.3	Захранващ модул	CP-E 24/2.5	2
2.5.4	Лиценз	PLC/Archives License, SD-card	2

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

2.5.5	Клеми – 18 пина	23XS40 R3001	30
2.5.6	Кабелни накрайници	23XS40 R4001	540

№	КОНФИГУРАЦИЯ НА RTU	ТИП RTU / МОДУЛ	БРОЙ
3.	**„SAS комуникационен сървър“**		
3.1.	Шкаф	ЕЛ -ТЕСТ -2200/800/800	1
3.2.	Шаси	560SFR02 R0001	1
3.2.1.	Общ брой слотове	Вградени в шасито	21
3.3.	Модули:		
3.3.1.	захранващ модул	560PSR00 R0001	2
3.3.2.	процесорен модул	560CMR02 R0001	4
3.3.3.	комуникационен модул	Вграден в процесорния модул	4
3.3.4.	модул цифрови входове	560BIR01 R0001	1
3.3.5.	модул аналогови входове	560AIR01 R0001	2
3.3.6.	модул цифрови изходи-сигнали	560BOR01 R0002	0
3.3.7.	модул цифрови изходи-команди	560BOR01 R0002	1
3.3.8.	модул аналогови изходи	23AA21 R0001	0
3.3.9.	модул входове цифрово измерване (BCD code)	560BIR01 R0001	1
3.4	Интерфейсни кабели за входни-изходните модули до репартитор (15 метра всеки)	TCBB 10x2x0,5	5
3.5	Други		

3.5.1	Връзка за процесна шина	560BCU05 R0001	1
3.5.2	Връзка за процесна шина	560BCU05 R1002	1
3.5.3	Захранващ модул	CP-E 24/2.5	1
3.5.4	Лиценз	PLC/Archives License, SD-card	4
3.5.5	Клеми – 18 пина	23XS40 R3001	9
3.5.6	Кабелни накрайници	23XS40 R4001	162

Обяснения към Таблица В:

- **Изисква се резервиране на захранването на RTU** (по изискванията на т.3.3 от Раздел Б. „Технически спецификации"). При единична повреда по захранващите вериги/модули не трябва да се стига до отпадане на: цялото RTU, комуникациите към диспечерските центрове на ЦДУ/ТДУ, комуникациите с интелигентните устройства в обекта както и отпадане на цифрови входове, цифрови изходи и аналогави входове.
- **Всички предложени конфигурации трябва да имат минимум два свободни слота за модули с входно-изходни интерфейси.**
- **Участникът да опише в Таблица В всички включени в конфигурацията типове модули**, които представляват обособена част за замяна и разширение, за да могат да се включват такива модули в заявки за доставка. Ако не е предвиден ред за тях, то такъв да се допълни като подпозиция на графа „Други".
- Стандартни материали (клеми, предпазители и др.), използвани при асемблиране на отделните модули до готово RTU ще се считат за включени в шкафа.
- Ако предложените конфигурации включват няколко шасита (или самостоятелни устройства), то включените във всяко шаси (или самостоятелно устройство) модули да се опишат отделно (повтаряйки съответните позиции X.2.x и X.3.x от таблица **Таблица В** необходимия брой пъти) като по този начин ще е възможно поръчката на оборудвано в такава конфигурация шаси
- Допустимо е един модул да комбинира няколко функции.

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

Документ 4.4.

Попълнена Таблица Г „Съответствията на RTU с минималните изисквания на Възложителя“ към т. А.2 от раздел I от докуметцията за участие, като се спазват указанията към тази таблица.

ТАБЛИЦА Г Съответствията на RTU с минималните изисквания на Възложителя

Таблица Г – Конфигурация „Голям

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
1	**СТАНДАРТИ (ИЛИ ТЕХНИ ЕКВИВАЛЕНТИ)**		
	- стандарт за качество	БДС EN ISO 9001	БДС EN ISO 9001
	- стандартно напрежение	БДС EN 60038	БДС EN 60038
	- степен на защита (IP) БДС EN 60529	IP 41	IP 41
	- Защитеност от пренапрежение БДС EN 60870-2-1 A2.2 level 3 (≥2 kVp)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от бързи преходни процеси БДС EN 60870-2-1 A2.3 level 3 (≥2 kVp)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от електростатично електричество БДС EN 60870-2-1 A3.1 level 3 (≥ 6 kV)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от електромагнитно поле БДС EN 60870-2-1 A5.1 level3 (≥10V/m)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от смущения, предизвикани от радиочестотни полета БДС EN 61000-4-6 level 3 (10 V)	Да покрива критерии „А"	Покрива критерии „А"
	- Ниво на галванична изолация между захранващи, комуникационни и сигнални интерфейси – 50Hz	БДС EN 60870-2-1 class VW3 (2,5kVrms - 60sec)	БДС EN 60870-2-1 class VW3 (2,5kVrms - 60sec)
	- Ниво на галванична изолация между захранващи, комуникационни и сигнални интерфейси – импулсно	БДС EN 60870-2-1 class VW3 (5kV – 1,2/50μsec)	БДС EN 60870-2-1 class VW3 (5kV – 1,2/50μsec)
2	**ОБЩИ ИЗИСКВАНИЯ**		
2.1.	Материали	Съответства на изискванията на т.Б.2.1.	Съответства на изискванията на т.Б.2.1.
2.2.	Модерни технологии	Съответства на изискванията на т.Б.2.2.	Съответства на изискванията на т.Б.2.2.

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
2.3.	Компоненти	Съответства на изискванията на т.Б.2.3.	Съответства на изискванията на т.Б.2.3.
2.4.	Функционални изисквания		
	Надеждност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Достъпност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Лесна поддръжка	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Изискване за безопасност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Проектен живот на системата	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Поддръжка на различни нива на резервираност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Маркировка - на всеки отделен модул, платка, кабел, ... - език – Български или английски - материали, издържливи на износване	 Да Да Да	 Да Да Да
2.5.	Климатични условия - вътрешни климатични условия температура ^{0}C влажност при 23^{0}C %	 +0 ÷ +50 или по-широк обхват 20 ÷ 90 или по-широк обхват	 -25 ÷ +55 5 ÷ 95
3	**ТЕХНИЧЕСКИ ИЗИСКВАНИЯ към RTU**		
3.1.	**Общи технически изисквания**		
	Конфигурация на RTU	Да се посочи	„Голям“

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	Производител	Да се посочи	ABB AG
	Разполагаемост (изчислена по приложената методика)	≥ 0,9975	0.9999934
	Памет за конфигурация и за архиви	Независими от електрозахранване	Независими от електрозахранване
	Комплектност на доставката	Съответства на изискванията на т.Б.3.1	Съответства на изискванията на т.Б.3.1
3.2.	**Функционални изисквания**		
3.2.1.	**Системни функции**		
	Телеуправление		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телерегулиране		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телесигнализация		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телеизмерване		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телеброене		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Цифрово измерване		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			техническа документация
	Поддържане на събития и аларми		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Буферите да съхраняват събитията при отпадане на връзката с горно ниво – бр. събития за комуникационна линия	≥500	10000
	Синхронизация на астрономическото време		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	- Протокол за получаване на астрономическо време	(S)NTP, IEC 60870-5-101	(S)NTP, IEC 60870-5-101
	- Протокол за сверяване на астрономическо време на локални устройства	(S)NTP, IEC60870-5-101, IEC60870-5-103	(S)NTP, IEC60870-5-101, IEC60870-5-103
	Комуникации		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Резервираност		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Архитектура		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Функции свързани със сигурност		
	Съответства на изискванията на т. Б.3.2.1	Да	Да, съгласно приложената

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			техническа документация
	Самодиагностика		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
3.2.2.	**Функционални изисквания към модулите на RTU**		
	Общи изисквания		
	- конфигурация, изградена на модулен принцип	Да	Да, съгласно приложената техническа документация
	- галванично разделени входове и изходи	Да	Да, съгласно приложената техническа документация
	- монтаж на модулите в шаси	Да	Да, съгласно приложената техническа документация
	Допустим толеранс на захранващо напрежение 230VAC, 50 Hz	+10/-15%, или по-широк	+10/-15%
	Допустим толеранс на захранващо напрежение 220VDC	+15/-20%, или по-широк	+15/-20%
	Допустим толеранс на захранващо напрежение 48VDC	+20/-10%, или по-широк	+20/-10%
	Липса на системи за принудително охлаждане, включително и на захранващите блокове.	Да	Да, съгласно приложената техническа документация
	Цифрови входове		
	- тип на предложения модул	Да се посочи	560BIR01 R0001
	- брой цифрови входове в един модул	Да се посочи	16
	- обработка на единични и двойни сигнализации	Да	Да, съгласно приложената

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			техническа документация
	- обработка на броячни стойности	Да	Да, съгласно приложената техническа документация
	- обработка на битова последователност	Да	Да, съгласно приложената техническа документация
	- апаратно и програмно филтриране на смущенията	Да	Да, съгласно приложената техническа документация
	- разделителна способност на времето за хронологичните събития	≤1ms	1ms
	- използуват се потенциално свободни контакти	Да	Да, съгласно приложената техническа документация
	- помощно напрежение	Unom.=48 VDC	Unom.=48 VDC
	- минимален обхват на входно напрежение за „логическа 0“	в интервал 0-7 VDC	в интервал 0-7 VDC
	- минимален обхват на входно напрежение за „логическа 1“	в интервал 20-48 VDC	в интервал 20-48 VDC
	- отчитане на импулси за ТБ с дължина:	≤40 msec	1 msec
	Аналогови входове		
	- тип на предложения модул	Да се посочи	560AIR01 R0001
	- брой аналогови входове в един модул	Да се посочи	8
	- грешка при измерване	≤0,2%	0.2 %
	- цикъл на сканиране за ТИ секунди	≤1	0.486
	- възможност за конфигуриране аналогови входове в обхвати -20÷20mA, ±5 mA и 4÷20 mA	Да	Да, съгласно приложената техническа документация

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	- разрядност на АЦП	минимум 11бита стойност + 1 бит знак;	12 бита стойност + 1 бит знак
	Цифрови изходи		
	Цифрови изходи за команди		
	- тип на предложения модул за команди	Да се посочи	560BOR01 R0002
	- брой цифрови изходи в един модул за команди	Да се посочи	16
	- изпълнение на единични и двойни команди	Да	Да, съгласно приложената техническа документация
	- проверка достоверността на Т К.	Да	Да, съгласно приложената техническа документация
	- проверка на изпълнението на условията за активиране на ТК	Да	Да, съгласно приложената техническа документация
	- регулиране продължителността на ТК	Да	Да, съгласно приложената техническа документация
	- помощно напрежение	48 VDC	48 VDC
	Цифрови изходи за сигнали		
	- тип на предложения модул за сигнали	Да се посочи	560BOR01 R0002
	- брой цифрови изходи в един модул за сигнали	Да се посочи	16
	- помощно напрежение	48 VDC	48 VDC
	- регулиране продължителността на сигнали "Строб" / "Валидно"	Да	Да, съгласно приложената техническа документация
	Аналогови изходи		

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	- тип на предложения модул	Да се посочи	23AA21 R0001
	- брой аналогови изходи в един модул	Да се посочи	2
	- обхват с възможност за конфигуриране 0÷5mA, 0÷20mA и 4÷20 mA	Да	Да, съгласно приложената техническа документация
	- разрядност на ЦАП	≥ 11 бита;	11 бита
	Комуникации с контролни центрове		
	Максимално поддържан брой комуникации с контролни центрове	≥ 4	4
	- тип на предложения комуникационен модул	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул	Да се посочи	8
	- протокол за обмен на телеинформация с контролни центрове съгласно IEC60870-5-101 - slave	Да	Да, съгласно приложената техническа документация
	- тип на интерфейса	RS 232	RS 232
	- протокол за обмен на телеинформация с контролни центрове съгласно IEC60870-5-104 - server	Да	Да, съгласно приложената техническа документация
	- протокол за обмен на телеинформация с контролни центрове съгласно Secured IEC60870-5-104 - server съгласно IEC 62351-3	Да	Да, съгласно приложената техническа документация
	- тип на интерфейса	Ethernet	Ethernet
	- възможност за разширяване броя на потребителите	Да	Да, съгласно приложената техническа документация
	Комуникации с устройства в рамките на обекта		

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	поддръжка на протокол IEC 61850 Ed.1 и Ed.2 (client), съгласно Приложение 9	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC 61850	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC 61850	Да се посочи	2
	- тип на интерфейса за комуникация по протокол IEC 61850	Ethernet оптичен или електрически	Ethernet електрически RJ45
	поддръжка на протокол IEC60870-5-104 (client and server)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC60870-5-104	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC60870-5-104	Да се посочи	2
	- тип на интерфейса за комуникация по протокол IEC60870-5-104	Ethernet	Ethernet
	поддръжка на протокол IEC60870-5-103 (master)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC60870-5-103	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC60870-5-103	Да се посочи	6
	- тип на интерфейса за комуникация по протокол IEC60870-5-103	Да се посочи	RS232C или RS485

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	поддръжка на протокол IEC60870-5-101 (master and slave)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC60870-5-101	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC60870-5-101	Да се посочи	6
	- тип на интерфейса за комуникация по протокол IEC60870-5-101	RS 232	RS 232
	поддръжка на протокол Modbus/RTU (master)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол Modbus/RTU	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол Modbus/RTU	Да се посочи	6
	- тип на интерфейса за комуникация по протокол Modbus/RTU	Да се посочи	RS232C или RS485
3.2.3.	**Система за конфигуриране на RTU RTU Configuration System**		
	- да изпълнява следните функции		
	➢ конфигуриране на системата	Да	Да, съгласно приложената техническа документация
	➢ тестване на системата	Да	Да, съгласно приложената техническа документация

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	➢ въвеждане в експлоатация на системата	Да	Да, съгласно приложената техническа документация
	➢ съхраняване на SW документация на системата	Да	Да, съгласно приложената техническа документация
	➢ създаване и модифициране на базата данни	Да	Да, съгласно приложената техническа документация
	➢ зареждане на базата данни и програмите	Да	Да, съгласно приложената техническа документация
	➢ конфигуриране на броя и вида на интелигентни електронни устройства	Да	Да, съгласно приложената техническа документация
	➢ програмиране на логики: блокировки, суми на логически сигнали, суми на стойности на измервания и др.	Да	Да, съгласно приложената техническа документация
	➢ конфигуриране на филтъра за измерваните и изчислени аналогови величини	Да	Да, съгласно приложената техническа документация
	➢ вход в системата с парола за достъп	Да	Да, съгласно приложената техническа документация
	➢ дистанционно конфигуриране, тестване и наблюдение	Да	Да, съгласно приложената техническа документация
	➢ сигурност при при дистанционен достъп	Да се посочи използвания способ	• HTTPS web server access – изпратената

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			информация е криптирана • Потребителско име/Парола – не е възможен достъп без оторизация • Достъп според ролята (RBAC) – достъпът е ограничен на принципа минимално необходимото да се знае. • VPN – може да се използват криптирани информационни тунели • Работа със сертификати – само устройства с валидни сертификати получават достъп до комуникациите в мрежата • Комуникационен стандарт Secure 104 – криптиране на информацията по IEC104
	- тип на интерфейса към RTU	Да се посочи	• 6x serial communication interface (RS-232 or RS-485) for

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			remote communication • 2x Ethernet interface (10/100BaseT) • 1x USB port • 1x serial peripheral bus
	- скорост на връзката към RTU	Да се посочи	• USB 2.0 - max. 480 MBit/s • Ethernet communication: 10-100 Mbit/s • RS232C: bitrate 200 bit/s - 38.4 kbit/s • RS485: bitrate 200 bit/s - 38.4 kbit/s
	Системни изисквания към работни станции - Съответства на изискванията на на т.Б.3.2.3.1	Да	Да, съгласно приложената техническа документация
3.2.4.	**Функционални изисквания към шкаф за RTU**		
	Съответства на изискванията на на т.Б.3.2.4.	Да	Да, съгласно приложената техническа документация
3.3.	**Параметри на системата**		
	- изпълнява минималните изисквания на сигналите за самодиагностика на т.Б.3.3.	Да	Да, съгласно приложената техническа документация
	- съответствие с приложения Interoperability list за IEC 60870-5-101 - Приложение 3.	Да	Да, съгласно приложената техническа документация

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	- съответствие с приложения Interoperability list за IEC 60870-5-104 - Приложение 4.	Да	Да, съгласно приложената техническа документация
	- съответствие с приложения Interoperability list за IEC 60870-5-103 - Приложение 5.	Да	Да, съгласно приложената техническа документация
	- съответствие с приложения Interoperability list за Modbus/RTU - Приложение 6.	Да	Да, съгласно приложената техническа документация
4.	**Тестове**		
4.1	**Заводски приемни изпитания**		
	Предложението съответства на изискванията на т.А.3.4.1	Да	Да
4.2	**Въвеждане в експлоатация на RTU в п/ст „Елин Пелин“, п/ст „Бабово“ и п/ст „Капитан Петко“**		
	Предложението съответства на изискванията на т.А.3.4.2	Да	Да
5.	**Документация**		
	Предложението съответства на изискванията на т.А.3.5.	Да	Да
6.	**Изискване към апаратурата**		
	Предложението съответства на изискванията на т.А.3.6	Да	Да
7.	**Гаранционен срок и гаранционно поддържане**		
	Предложението съответства на изискванията на т.А.4	Да	Да
8.	**Функционални изисквания към обучение**		
	Предложеното обучение съответства на изискванията на т.А.5	Да	Да
9.	**Консултации**		
	Предложението съот ветства на изискванията на т.А.6.	Да	Да

Таблица Г за конфигурация „Малък“

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
1	**СТАНДАРТИ (ИЛИ ТЕХНИ ЕКВИВАЛЕНТИ)**		
	- стандарт за качество	БДС EN ISO 9001	БДС EN ISO 9001
	- стандартно напрежение	БДС EN 60038	БДС EN 60038
	- степен на защита (IP) БДС EN 60529	IP 41	IP 41
	- Защитеност от пренапрежение БДС EN 60870-2-1 A2.2 level 3 (≥2 kVp)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от бързи преходни процеси БДС EN 60870-2-1 A2.3 level 3 (≥2 kVp)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от електростатично електричество БДС EN 60870-2-1 A3.1 level 3 (≥ 6 kV)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от електромагнитно поле БДС EN 60870-2-1 A5.1 level3 (≥10V/m)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от смущения, предизвикани от радиочестотни полета БДС EN 61000-4-6 level 3 (10 V)	Да покрива критерии „А"	Покрива критерии „А"
	- Ниво на галванична изолация между захранващи, комуникационни и сигнални интерфейси – 50Hz	БДС EN 60870-2-1 class VW3 (2,5kVrms - 60sec)	БДС EN 60870-2-1 class VW3 (2,5kVrms - 60sec)
	- Ниво на галванична изолация между захранващи, комуникационни и сигнални интерфейси – импулсно	БДС EN 60870-2-1 class VW3 (5kV – 1,2/50μsec)	БДС EN 60870-2-1 class VW3 (5kV – 1,2/50μsec)
2	**ОБЩИ ИЗИСКВАНИЯ**		
2.1.	Материали	Съответства на изискванията на т.Б.2.1.	Съответства на изискванията на т.Б.2.1.
2.2.	Модерни технологии	Съответства на изискванията на т.Б.2.2.	Съответства на изискванията на т.Б.2.2.

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
2.3.	Компоненти	Съответства на изискванията на т.Б.2.3.	Съответства на изискванията на т.Б.2.3.
2.4.	Функционални изисквания		
	Надеждност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Достъпност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Лесна поддръжка	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Изискване за безопасност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Проектен живот на системата	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Поддръжка на различни нива на резервираност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Маркировка - на всеки отделен модул, платка, кабел, ... - език – Български или английски - материали, издържливи на износване	 Да Да Да	 Да Да Да
2.5.	Климатични условия - вътрешни климатични условия температура ^{0}C влажност при 23^{0}C %	 +0 ÷ +50 или по-широк обхват 20 ÷ 90 или по-широк обхват	 -25 ÷ +55 5 ÷ 95
3	**ТЕХНИЧЕСКИ ИЗИСКВАНИЯ към RTU**		
3.1.	**Общи технически изисквания**		
	Конфигурация на RTU	Да се посочи	„Малък“

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	Производител	Да се посочи	ABB AG
	Разполагаемост (изчислена по приложената методика)	≥ 0,9975	0.9999906
	Памет за конфигурация и за архиви	Независими от електрозахранване	Независими от електрозахранване
	Комплектност на доставката	Съответства на изискванията на т.Б.3.1	Съответства на изискванията на т.Б.3.1
3.2.	**Функционални изисквания**		
3.2.1.	**Системни функции**		
	Телеуправление		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телерегулиране		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телесигнализация		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телеизмерване		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телеброене		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Цифрово измерване		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			техническа документация
	Поддържане на събития и аларми		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Буферите да съхраняват събитията при отпадане на връзката с горно ниво – бр. събития за комуникационна линия	≥500	10000
	Синхронизация на астрономическото време		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	- Протокол за получаване на астрономическо време	(S)NTP, IEC 60870-5-101	(S)NTP, IEC 60870-5-101
	- Протокол за сверяване на астрономическо време на локални устройства	(S)NTP, IEC60870-5-101, IEC60870-5-103	(S)NTP, IEC60870-5-101, IEC60870-5-103
	Комуникации		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Резервираност		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Архитектура		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Функции свързани със сигурност		
	Съответства на изискванията на т. Б.3.2.1	Да	Да, съгласно приложената

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			техническа документация
	Самодиагностика		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
3.2.2.	**Функционални изисквания към модулите на RTU**		
	Общи изисквания		
	- конфигурация, изградена на модулен принцип	Да	Да, съгласно приложената техническа документация
	- галванично разделени входове и изходи	Да	Да, съгласно приложената техническа документация
	- монтаж на модулите в шаси	Да	Да, съгласно приложената техническа документация
	Допустим толеранс на захранващо напрежение 230VAC, 50 Hz	+10/-15%, или по-широк	+10/-15%
	Допустим толеранс на захранващо напрежение 220VDC	+15/-20%, или по-широк	+15/-20%
	Допустим толеранс на захранващо напрежение 48VDC	+20/-10%, или по-широк	+20/-10%
	Липса на системи за принудително охлаждане, включително и на захранващите блокове.	Да	Да, съгласно приложената техническа документация
	Цифрови входове		
	- тип на предложения модул	Да се посочи	560BIR01 R0001
	- брой цифрови входове в един модул	Да се посочи	16
	- обработка на единични и двойни сигнализации	Да	Да, съгласно приложената

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			техническа документация
	- обработка на броячни стойности	Да	Да, съгласно приложената техническа документация
	- обработка на битова последователност	Да	Да, съгласно приложената техническа документация
	- апаратно и програмно филтриране на смущенията	Да	Да, съгласно приложената техническа документация
	- разделителна способност на времето за хронологичните събития	≤1ms	1ms
	- използуват се потенциално свободни контакти	Да	Да, съгласно приложената техническа документация
	- помощно напрежение	Unom.=48 VDC	Unom.=48 VDC
	- минимален обхват на входно напрежение за „логическа 0“	в интервал 0-7 VDC	в интервал 0-7 VDC
	- минимален обхват на входно напрежение за „логическа 1“	в интервал 20-48 VDC	в интервал 20-48 VDC
	- отчитане на импулси за ТБ с дължина:	≤40 msec	1 msec
	Аналогови входове		
	- тип на предложения модул	Да се посочи	560AIR01 R0001
	- брой аналогови входове в един модул	Да се посочи	8
	- грешка при измерване	≤0,2%	0.2 %
	- цикъл на сканиране за ТИ секунди	≤1	0.486
	- възможност за конфигуриране аналогови входове в обхвати -20÷20mA, ±5 mA и 4÷20 mA	Да	Да, съгласно приложената техническа документация

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	- разрядност на АЦП	минимум 11бита стойност + 1 бит знак;	12 бита стойност + 1 бит знак
	Цифрови изходи		
	Цифрови изходи за команди		
	- тип на предложения модул за команди	Да се посочи	560BOR01 R0002
	- брой цифрови изходи в един модул за команди	Да се посочи	16
	- изпълнение на единични и двойни команди	Да	Да, съгласно приложената техническа документация
	- проверка достоверността на Т К.	Да	Да, съгласно приложената техническа документация
	- проверка на изпълнението на условията за активиране на ТК	Да	Да, съгласно приложената техническа документация
	- регулиране продължителността на ТК	Да	Да, съгласно приложената техническа документация
	- помощно напрежение	48 VDC	48 VDC
	Цифрови изходи за сигнали		
	- тип на предложения модул за сигнали	Да се посочи	560BOR01 R0002
	- брой цифрови изходи в един модул за сигнали	Да се посочи	16
	- помощно напрежение	48 VDC	48 VDC
	- регулиране продължителността на сигнали "Строб" / "Валидно"	Да	Да, съгласно приложената техническа документация
	Аналогови изходи		

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	- тип на предложения модул	Да се посочи	23AA21 R0001
	- брой аналогови изходи в един модул	Да се посочи	2
	- обхват с възможност за конфигуриране 0÷5mA, 0÷20mA и 4÷20 mA	Да	Да, съгласно приложената техническа документация
	- разрядност на ЦАП	≥ 11 бита;	11 бита
	Комуникации с контролни центрове		
	Максимално поддържан брой комуникации с контролни центрове	≥ 4	4
	- тип на предложения комуникационен модул	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул	Да се посочи	8
	- протокол за обмен на телеинформация с контролни центрове съгласно IEC60870-5-101 - slave	Да	Да, съгласно приложената техническа документация
	- тип на интерфейса	RS 232	RS 232
	- протокол за обмен на телеинформация с контролни центрове съгласно IEC60870-5-104 - server	Да	Да, съгласно приложената техническа документация
	- протокол за обмен на телеинформация с контролни центрове съгласно Secured IEC60870-5-104 - server съгласно IEC 62351-3	Да	Да, съгласно приложената техническа документация
	- тип на интерфейса	Ethernet	Ethernet
	- възможност за разширяване броя на потребителите	Да	Да, съгласно приложената техническа документация
	Комуникации с устройства в рамките на обекта		

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	поддръжка на протокол IEC 61850 Ed.1 и Ed.2 (client), съгласно Приложение 9	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC 61850	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC 61850	Да се посочи	2
	- тип на интерфейса за комуникация по протокол IEC 61850	Ethernet оптичен или електрически	Ethernet електрически RJ45
	поддръжка на протокол IEC60870-5-104 (client and server)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC60870-5-104	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC60870-5-104	Да се посочи	2
	- тип на интерфейса за комуникация по протокол IEC60870-5-104	Ethernet	Ethernet
	поддръжка на протокол IEC60870-5-103 (master)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC60870-5-103	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC60870-5-103	Да се посочи	6
	- тип на интерфейса за комуникация по протокол IEC60870-5-103	Да се посочи	RS232C или RS485

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	поддръжка на протокол IEC60870-5-101 (master and slave)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC60870-5-101	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC60870-5-101	Да се посочи	6
	- тип на интерфейса за комуникация по протокол IEC60870-5-101	RS 232	RS 232
	поддръжка на протокол Modbus/RTU (master)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол Modbus/RTU	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол Modbus/RTU	Да се посочи	6
	- тип на интерфейса за комуникация по протокол Modbus/RTU	Да се посочи	RS232C или RS485
3.2.3.	**Система за конфигуриране на RTU RTU Configuration System**		
	- да изпълнява следните функции		
	➢ конфигуриране на системата	Да	Да, съгласно приложената техническа документация
	➢ тестване на системата	Да	Да, съгласно приложената техническа документация

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	➢ въвеждане в експлоатация на системата	Да	Да, съгласно приложената техническа документация
	➢ съхраняване на SW документация на системата	Да	Да, съгласно приложената техническа документация
	➢ създаване и модифициране на базата данни	Да	Да, съгласно приложената техническа документация
	➢ зареждане на базата данни и програмите	Да	Да, съгласно приложената техническа документация
	➢ конфигуриране на броя и вида на интелигентни електронни устройства	Да	Да, съгласно приложената техническа документация
	➢ програмиране на логики: блокировки, суми на логически сигнали, суми на стойности на измервания и др.	Да	Да, съгласно приложената техническа документация
	➢ конфигуриране на филтъра за измерваните и изчислени аналогови величини	Да	Да, съгласно приложената техническа документация
	➢ вход в системата с парола за достъп	Да	Да, съгласно приложената техническа документация
	➢ дистанционно конфигуриране, тестване и наблюдение	Да	Да, съгласно приложената техническа документация
	➢ сигурност при при дистанционен достъп	Да се посочи използвания способ	• HTTPS web server access – изпратената

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			информация е криптирана • Потребителско име/Парола – не е възможен достъп без оторизация • Достъп според ролята (RBAC) – достъпът е ограничен на принципа минимално необходимото да се знае. • VPN – може да се използват криптирани информационни тунели • Работа със сертификати – само устройства с валидни сертификати получават достъп до комуникациите в мрежата • Комуникационен стандарт Secure 104 – криптиране на информацията по IEC104
	- тип на интерфейса към RTU	Да се посочи	• 6x serial communication interface (RS-232 or RS-485) for

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			remote communication • 2x Ethernet interface (10/100BaseT) • 1x USB port • 1x serial peripheral bus
	- скорост на връзката към RTU	Да се посочи	• USB 2.0 - max. 480 MBit/s • Ethernet communication: 10-100 Mbit/s • RS232C: bitrate 200 bit/s - 38.4 kbit/s • RS485: bitrate 200 bit/s - 38.4 kbit/s
	Системни изисквания към работни станции - Съответства на изискванията на на т.Б.3.2.3.1	Да	Да, съгласно приложената техническа документация
3.2.4.	**Функционални изисквания към шкаф за RTU**		
	Съответства на изискванията на на т.Б.3.2.4.	Да	Да, съгласно приложената техническа документация
3.3.	**Параметри на системата**		
	- изпълнява минималните изисквания на сигналите за самодиагностика на т.Б.3.3.	Да	Да, съгласно приложената техническа документация
	- съответствие с приложения Interoperability list за IEC 60870-5-101 - Приложение 3.	Да	Да, съгласно приложената техническа документация

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	- съответствие с приложения Interoperability list за IEC 60870-5-104 - Приложение 4.	Да	Да, съгласно приложената техническа документация
	- съответствие с приложения Interoperability list за IEC 60870-5-103 - Приложение 5.	Да	Да, съгласно приложената техническа документация
	- съответствие с приложения Interoperability list за Modbus/RTU - Приложение 6.	Да	Да, съгласно приложената техническа документация
4.	**Тестове**		
4.1	**Заводски приемни изпитания**		
	Предложението съответства на изискванията на т.А.3.4.1	Да	Да
4.2	**Въвеждане в експлоатация на RTU в п/ст „Елин Пелин", п/ст „Бабово" и п/ст „Капитан Петко"**		
	Предложението съответства на изискванията на т.А.3.4.2	Да	Да
5.	**Документация**		
	Предложението съответства на изискванията на т.А.3.5.	Да	Да
6.	**Изискване към апаратурата**		
	Предложението съответства на изискванията на т.А.3.6	Да	Да
7.	**Гаранционен срок и гаранционно поддържане**		
	Предложението съответства на изискванията на т.А.4	Да	Да
8.	**Функционални изисквания към обучение**		
	Предложеното обучение съответства на изискванията на т.А.5	Да	Да
9.	**Консултации**		
	Предложението съот ветства на изискванията на т.А.6.	Да	Да

Таблица Г за конфигурация SAS Комуникационен сървър

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
1	**СТАНДАРТИ (ИЛИ ТЕХНИ ЕКВИВАЛЕНТИ)**		
	- стандарт за качество	БДС EN ISO 9001	БДС EN ISO 9001
	- стандартно напрежение	БДС EN 60038	БДС EN 60038
	- степен на защита (IP) БДС EN 60529	IP 41	IP 41
	- Защитеност от пренапрежение БДС EN 60870-2-1 A2.2 level 3 (≥2 kVp)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от бързи преходни процеси БДС EN 60870-2-1 A2.3 level 3 (≥2 kVp)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от електростатично електричество БДС EN 60870-2-1 A3.1 level 3 (≥ 6 kV)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от електромагнитно поле БДС EN 60870-2-1 A5.1 level3 (≥10V/m)	Да покрива критерии „А"	Покрива критерии „А"
	- Защитеност от смущения, предизвикани от радиочестотни полета БДС EN 61000-4-6 level 3 (10 V)	Да покрива критерии „А"	Покрива критерии „А"
	- Ниво на галванична изолация между захранващи, комуникационни и сигнални интерфейси – 50Hz	БДС EN 60870-2-1 class VW3 (2,5kVrms - 60sec)	БДС EN 60870-2-1 class VW3 (2,5kVrms - 60sec)
	- Ниво на галванична изолация между захранващи, комуникационни и сигнални интерфейси – импулсно	БДС EN 60870-2-1 class VW3 (5kV – 1,2/50μsec)	БДС EN 60870-2-1 class VW3 (5kV – 1,2/50μsec)
2	**ОБЩИ ИЗИСКВАНИЯ**		
2.1.	Материали	Съответства на изискванията на т.Б.2.1.	Съответства на изискванията на т.Б.2.1.
2.2.	Модерни технологии	Съответства на изискванията на т.Б.2.2.	Съответства на изискванията на т.Б.2.2.

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
2.3.	Компоненти	Съответства на изискванията на т.Б.2.3.	Съответства на изискванията на т.Б.2.3.
2.4.	Функционални изисквания		
	Надеждност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Достъпност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Лесна поддръжка	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Изискване за безопасност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Проектен живот на системата	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Поддръжка на различни нива на резервираност	Съответства на изискванията на т.Б.2.4.	Съответства на изискванията на т.Б.2.4.
	Маркировка - на всеки отделен модул, платка, кабел, ... - език – Български или английски - материали, издържливи на износване	 Да Да Да	 Да Да Да
2.5.	Климатични условия - вътрешни климатични условия температура ^{0}C влажност при 23^{0}C %	 +0 ÷ +50 или по-широк обхват 20 ÷ 90 или по-широк обхват	 -25 ÷ +55 5 ÷ 95
3	**ТЕХНИЧЕСКИ ИЗИСКВАНИЯ към RTU**		
3.1.	**Общи технически изисквания**		

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	Конфигурация на RTU	Да се посочи	„SAS Комуникационен сървър“
	Производител	Да се посочи	ABB AG
	Разполагаемост (изчислена по приложената методика)	≥ 0,9975	0.9999889
	Памет за конфигурация и за архиви	Независими от електрозахранване	Независими от електрозахранване
	Комплектност на доставката	Съответства на изискванията на т.Б.3.1	Съответства на изискванията на т.Б.3.1
3.2.	**Функционални изисквания**		
3.2.1.	**Системни функции**		
	Телеуправление		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телерегулиране		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телесигнализация		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телеизмерване		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Телеброене		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	Цифрово измерване		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Поддържане на събития и аларми		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Буферите да съхраняват събитията при отпадане на връзката с горно ниво – бр. събития за комуникационна линия	≥500	10000
	Синхронизация на астрономическото време		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	- Протокол за получаване на астрономическо време	(S)NTP, IEC 60870-5-101	(S)NTP, IEC 60870-5-101
	- Протокол за сверяване на астрономическо време на локални устройства	(S)NTP, IEC60870-5-101, IEC60870-5-103	(S)NTP, IEC60870-5-101, IEC60870-5-103
	Комуникации		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Резервираност		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
	Архитектура		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	Функции свързани със сигурност		
	Съответства на изискванията на т. Б.3.2.1	Да	Да, съгласно приложената техническа документация
	Самодиагностика		
	Съответства на изискванията на т. Б.3.2.1.	Да	Да, съгласно приложената техническа документация
3.2.2.	**Функционални изисквания към модулите на RTU**		
	Общи изисквания		
	- конфигурация, изградена на модулен принцип	Да	Да, съгласно приложената техническа документация
	- галванично разделени входове и изходи	Да	Да, съгласно приложената техническа документация
	- монтаж на модулите в шаси	Да	Да, съгласно приложената техническа документация
	Допустим толеранс на захранващо напрежение 230VAC, 50 Hz	+10/-15%, или по-широк	+10/-15%
	Допустим толеранс на захранващо напрежение 220VDC	+15/-20%, или по-широк	+15/-20%
	Допустим толеранс на захранващо напрежение 48VDC	+20/-10%, или по-широк	+20/-10%
	Липса на системи за принудително охлаждане, включително и на захранващите блокове.	Да	Да, съгласно приложената техническа документация
	Цифрови входове		
	- тип на предложения модул	Да се посочи	560BIR01 R0001
	- брой цифрови входове в един модул	Да се посочи	16

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

08.2017

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	- обработка на единични и двойни сигнализации	Да	Да, съгласно приложената техническа документация
	- обработка на броячни стойности	Да	Да, съгласно приложената техническа документация
	- обработка на битова последователност	Да	Да, съгласно приложената техническа документация
	- апаратно и програмно филтриране на смущенията	Да	Да, съгласно приложената техническа документация
	- разделителна способност на времето за хронологичните събития	≤1ms	1ms
	- използуват се потенциално свободни контакти	Да	Да, съгласно приложената техническа документация
	- помощно напрежение	Unom.=48 VDC	Unom.=48 VDC
	- минимален обхват на входно напрежение за „логическа 0"	в интервал 0-7 VDC	в интервал 0-7 VDC
	- минимален обхват на входно напрежение за „логическа 1"	в интервал 20-48 VDC	в интервал 20-48 VDC
	- отчитане на импулси за ТБ с дължина:	≤40 msec	1 msec
	Аналогови входове		
	- тип на предложения модул	Да се посочи	560AIR01 R0001
	- брой аналогови входове в един модул	Да се посочи	8
	- грешка при измерване	≤0,2%	0.2 %
	- цикъл на сканиране за ТИ секунди	≤1	0.486
	- възможност за конфигуриране аналогови входове в обхвати -20÷20mA, ±5 mA и 4÷20 mA	Да	Да, съгласно приложената техническа документация

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	- разрядност на АЦП	минимум 11бита стойност + 1 бит знак;	12 бита стойност + 1 бит знак
	Цифрови изходи		
	Цифрови изходи за команди		
	- тип на предложения модул за команди	Да се посочи	560BOR01 R0002
	- брой цифрови изходи в един модул за команди	Да се посочи	16
	- изпълнение на единични и двойни команди	Да	Да, съгласно приложената техническа документация
	- проверка достоверността на Т К.	Да	Да, съгласно приложената техническа документация
	- проверка на изпълнението на условията за активиране на ТК	Да	Да, съгласно приложената техническа документация
	- регулиране продължителността на ТК	Да	Да, съгласно приложената техническа документация
	- помощно напрежение	48 VDC	48 VDC
	Цифрови изходи за сигнали		
	- тип на предложения модул за сигнали	Да се посочи	Не е приложимо за тази конфигурация
	- брой цифрови изходи в един модул за сигнали	Да се посочи	Не е приложимо за тази конфигурация
	- помощно напрежение	48 VDC	48 VDC
	- регулиране продължителността на сигнали "Строб" / "Валидно"	Да	Да, съгласно приложената техническа документация

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	Аналогови изходи		
	- тип на предложения модул	Да се посочи	Не е приложимо за тази конфигурация
	- брой аналогови изходи в един модул	Да се посочи	Не е приложимо за тази конфигурация
	- обхват с възможност за конфигуриране 0÷5mA, 0÷20mA и 4÷20 mA	Да	Да, съгласно приложената техническа документация
	- разрядност на ЦАП	≥ 11 бита;	11 бита
	Комуникации с контролни центрове		
	Максимално поддържан брой комуникации с контролни центрове	≥ 4	4
	- тип на предложения комуникационен модул	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул	Да се посочи	8
	- протокол за обмен на телеинформация с контролни центрове съгласно IEC60870-5-101 - slave	Да	Да, съгласно приложената техническа документация
	- тип на интерфейса	RS 232	RS 232
	- протокол за обмен на телеинформация с контролни центрове съгласно IEC60870-5-104 - server	Да	Да, съгласно приложената техническа документация
	- протокол за обмен на телеинформация с контролни центрове съгласно Secured IEC60870-5-104 - server съгласно IEC 62351-3	Да	Да, съгласно приложената техническа документация
	- тип на интерфейса	Ethernet	Ethernet
	- възможност за разширяване броя на потребителите	Да	Да, съгласно приложената

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			техническа документация
	Комуникации с устройства в рамките на обекта		
	поддръжка на протокол IEC 61850 Ed.1 и Ed.2 (client), съгласно Приложение 9	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC 61850	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC 61850	Да се посочи	2
	- тип на интерфейса за комуникация по протокол IEC 61850	Ethernet оптичен или електрически	Ethernet електрически RJ45
	поддръжка на протокол IEC60870-5-104 (client and server)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC60870-5-104	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC60870-5-104	Да се посочи	2
	- тип на интерфейса за комуникация по протокол IEC60870-5-104	Ethernet	Ethernet
	поддръжка на протокол IEC60870-5-103 (master)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC60870-5-103	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за	Да се посочи	6

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	комуникация по протокол IEC60870-5-103		
	- тип на интерфейса за комуникация по протокол IEC60870-5-103	Да се посочи	RS232C или RS485
	поддръжка на протокол IEC60870-5-101 (master and slave)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол IEC60870-5-101	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол IEC60870-5-101	Да се посочи	6
	- тип на интерфейса за комуникация по протокол IEC60870-5-101	RS 232	RS 232
	поддръжка на протокол Modbus/RTU (master)	Да	Да, съгласно приложената техническа документация
	- тип на комуникационен модул за комуникация по протокол Modbus/RTU	Да се посочи	560CMR02 R0001
	- брой комуникационни интерфейси в един модул за комуникация по протокол Modbus/RTU	Да се посочи	6
	- тип на интерфейса за комуникация по протокол Modbus/RTU	Да се посочи	RS232C или RS485
3.2.3.	**Система за конфигуриране на RTU RTU Configuration System**		
	- да изпълнява следните функции		
	➢ конфигуриране на системата	Да	Да, съгласно приложената

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			техническа документация
	➢ тестване на системата	Да	Да, съгласно приложената техническа документация
	➢ въвеждане в експлоатация на системата	Да	Да, съгласно приложената техническа документация
	➢ съхраняване на SW документация на системата	Да	Да, съгласно приложената техническа документация
	➢ създаване и модифициране на базата данни	Да	Да, съгласно приложената техническа документация
	➢ зареждане на базата данни и програмите	Да	Да, съгласно приложената техническа документация
	➢ конфигуриране на броя и вида на интелигентни електронни устройства	Да	Да, съгласно приложената техническа документация
	➢ програмиране на логики: блокировки, суми на логически сигнали, суми на стойности на измервания и др.	Да	Да, съгласно приложената техническа документация
	➢ конфигуриране на филтъра за измерваните и изчислени аналогови величини	Да	Да, съгласно приложената техническа документация
	➢ вход в системата с парола за достъп	Да	Да, съгласно приложената техническа документация
	➢ дистанционно конфигуриране, тестване и наблюдение	Да	Да, съгласно приложената

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			техническа документация
	➢ сигурност при при дистанционен достъп	Да се посочи използвания способ	• HTTPS web server access – изпратената информация е криптирана • Потребителско име/Парола – не е възможен достъп без оторизация • Достъп според ролята (RBAC) – достъпът е ограничен на принципа минимално необходимото да се знае. • VPN – може да се използват криптирани информационни тунели • Работа със сертификати – само устройства с валидни сертификати получават достъп до комуникациите в мрежата • Комуникационен стандарт Secure 104 – криптиране на

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
			информацията по IEC104
	- тип на интерфейса към RTU	Да се посочи	• 6x serial communication interface (RS-232 or RS-485) for remote communication • 2x Ethernet interface (10/100BaseT) • 1x USB port • 1x serial peripheral bus
	- скорост на връзката към RTU	Да се посочи	• USB 2.0 - max. 480 MBit/s • Ethernet communication: 10-100 Mbit/s • RS232C: bitrate 200 bit/s - 38.4 kbit/s • RS485: bitrate 200 bit/s - 38.4 kbit/s
	Системни изисквания към работни станции - Съответства на изискванията на на т.Б.3.2.3.1	Да	Да, съгласно приложената техническа документация
3.2.4.	**Функционални изисквания към шкаф за RTU**		
	Съответства на изискванията на на т.Б.3.2.4.	Да	Да, съгласно приложената техническа документация
3.3.	**Параметри на системата**		
	- изпълнява минималните изисквания на сигналите за самодиагностика на т.Б.3.3.	Да	Да, съгласно приложената техническа документация

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	- съответствие с приложения Interoperability list за IEC 60870-5-101 - Приложение 3.	Да	Да, съгласно приложената техническа документация
	- съответствие с приложения Interoperability list за IEC 60870-5-104 - Приложение 4.	Да	Да, съгласно приложената техническа документация
	- съответствие с приложения Interoperability list за IEC 60870-5-103 - Приложение 5.	Да	Да, съгласно приложената техническа документация
	- съответствие с приложения Interoperability list за Modbus/RTU - Приложение 6.	Да	Да, съгласно приложената техническа документация
4.	**Тестове**		
4.1	**Заводски приемни изпитания**		
	Предложението съответства на изискванията на т.А.3.4.1	Да	Да
4.2	**Въвеждане в експлоатация на RTU в п/ст „Елин Пелин“, п/ст „Бабово“ и п/ст „Капитан Петко“**		
	Предложението съответства на изискванията на т.А.3.4.2	Да	Да
5.	**Документация**		
	Предложението съответства на изискванията на т.А.3.5.	Да	Да
6.	**Изискване към апаратурата**		
	Предложението съответства на изискванията на т.А.3.6	Да	Да
7.	**Гаранционен срок и гаранционно поддържане**		
	Предложението съответства на изискванията на т.А.4	Да	Да
8.	**Функционални изисквания към обучение**		

	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
	Предложеното обучение съответства на изискванията на т.А.5	Да	Да
9.	**Консултации**		
	Предложението съот ветства на изискванията на т.А.6.	Да	Да

Забележки:

1. Участникът трябва да попълни отделна ТАБЛИЦА Г НА СЪОТВЕТСТВИЯТА ЗА RTU **за всяка конфигурация** предложена апаратура, предмет на доставка и подлежаща на техническа оценка.

2. Участникът трябва да попълни **всички редове** от графа "Технически данни на Участника".

3. За редовете от таблицата, за които възложителят е посочил стойности „≤" или „≥", Участникът трябва да попълни конкретна стойност на съответните технически данни.

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

Документ 4.5.

Таблица в Приложение 1 от раздел I от документацията за участие – предложение, отговарящо на „Минималните изисквания към всяка конфигурация“

ПРИЛОЖЕНИЕ 1

Минималните изисквания към всяка конфигурация

№	Технически параметър / Характеристика		Конфигурация на RTU					
			Голям		Малък		SAS комуникационен сървър	
			Минимални изисквания на Възложителя	Предложение на участника	Минимални изисквания на Възложителя	Предложение на участника	Минимални изисквания на Възложителя	Предложение на участника
1.	Захранване на RTU							
1.1.	Основно захранване	AC и DC	220V (AC/DC)	220V (AC/DC)	220V (AC/DC)	220V (AC/DC)	220V (AC/DC)	220V (AC/DC)
1.2.	Резервно захранване	DC	48V (DC)	48V (DC)	48V (DC)	48V (DC)	48V (DC)	48V (DC)
2.	Аналогови входнове/изходи на RTU							
2.1.	Брой аналогови входове	AI	≥ 80	80	≥ 40	40	≥ 16	16
2.2.	Брой аналогови изходи	AO	≥ 4	4	≥ 4	4	≥ 0	0
3.	Цифрови входове/изходи на RTU							
3.1.	Брой цифрови входни сигнали	DI	≥ 360	368	≥ 240	240	≥ 16	16
3.2.	Брой цифрови входни Броячни сигнали	DI	≥ 8	16	≥ 8	16	≥ 0	0
3.3.	Брой цифрови входове за цифрово измерване (BCD code за стойности от 0 до 99)	BCD	≥ 2	2	≥ 2	2	≥ 2	2
3.4.	Брой цифрови изходи команди	CO	≥ 32	32	≥ 32	32	≥ 16	16
3.5.	Брой цифрови изходи Strobe/ Enable	DO	≥ 8	16	≥ 8	16	≥ 0	0
4.	Процесни точки на RTU							
4.1.	Общ брой процесни точки на RTU		≥ 5000	5000	≥ 2000	5000	≥ 5000	5000
5.	Връзка с контролни центрове на RTU							
5.1.	Брой контролни центрове		≥ 4	16	≥ 4	16	≥ 4	16
6.	Интерфейси на RTU							
6.1.	Общ брой Ethernet - интерфейси		≥ 4	4	≥ 4	4	≥ 8	8
6.1.1.	Брой Ethernet интерфейса - IEC 60870-5-104	Server/Client	≥ 2	2	≥ 2	2	≥ 4	4
6.1.2.	Брой Ethernet интерфейса - IEC 61850	Client	≥ 2	2	≥ 2	2	≥ 4	4
6.1.3.	Брой Ethernet Secured интерфейса - IEC 60870-5-104 съгл. IEC62351-3	Server/Client	≥ 2*	2	≥ 2*	2	≥ 2*	2

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

08.2017

6.2.	**Общ брой Serial - интерфейси**		≥ 6	12	≥ 6	12	≥ 10	24
6.2.1.	**Брой RS232 интерфейса - IEC 60870-5-101**	**Master/Slave***	≥ 3	3	≥2	2	≥2	2
6.2.2.	**Брой RS485 интерфейса - IEC 60870-5-103**	**Master**	≥ 1	1	≥2	2	≥6	6
6.2.3.	**Брой RS485 интерфейса - Modbus/RTU**	**Master**	≥ 2	2	≥2	2	≥2	2

*- Възможността за използване на secured IEC 60870-5-104 да е достъпна за активиране и деактивиране чрез системата за конфигуриране на RTU за посочения брой комуникационни протоколи. При невъзможност за изпълнение на предходното изискване, да се съобрази броя на „комуникационните интерфейси“, така, че да се изпълни условието за брой „Ethernet – комуникационни протоколи“.

АББ България ЕООД
Централен офис
бул. „Витоша“ № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

08.2017

Документи на CD

4.6. Описание на работа по протокол IEC 60870-5-101 (interoperability sheet), съответстваща на изискванията, описани в и на описаната в Приложение 3

4.7. Описание на работа по протокол IEC 60870-5-104 (interoperability sheet), съответстваща на изискванията, описани в Приложение 4

4.8. Описание на работа по протокол IEC 60870-5-103 (interoperability sheet), съответстваща на изискванията, описани в Приложение 5

4.9. Описание на работа по протокол Modbus/RTU (interoperability sheet), съответстваща на изискванията, описани в Приложение 6

4.12. Декларации от типа ACSI (Abstract Communication Service Interface), PICS (Protocol Implementation Conformance Statement), PIXIT (Protocol Implementation eXtra Information for Testing), MICS (Model Implementation Conformance Statement), TICS (Tissues Conformance Statement), Interoperability sheet, както е приложимо за поддържаните от RTU протоколи за комуникация.

4.13. Сертификати, издадени от акредитирани лица, удостоверяващи съответствието на телемеханичните системи от предлаганата серия със стандарти от сериите БДС EN 61850 Ed1, БДС EN 61850 Ed2, БДС EN 60870, БДС EN 62351-3 или техни еквиваленти

4.14. Схеми на цифрови входове, цифрови изходи, аналогови входове, аналогови изходи.

4.18. Описание на техническите характеристики на предлаганите от участника изделия. Представят се документи съдържащи техническа спецификация, като каталози, проспекти или технически данни на изделието.

Документи 4.10.

Таблица в Приложение 7 от раздел I от докуметацията за участие – Изисквания по стандарт за сигурност IEC 62351

ПРИЛОЖЕНИЕ 7

Изисквания по стандарт за сигурност IEC 62351

№	Технически характеристики и изисквания	Минимални изисквания на Възложителя	Техн. данни на Участника
1	**Кибер сигурност**		
1.1	Дефиниране на потребителски права и профили съгласно IEC 62351-8	Да	Да
1.2	Потребителски профили	≥25 бр.	25
1.3	Възможност за настройка на сложността на паролите:		
	-минимална дължина на паролата	≥8 символа	8 символа
	-наличие на малки и големи букви	Да	Да
	-наличие на цифри	Да	Да
	-наличие на специални символи	Да	Да
2.4	Списъци със събития отнасящи се до сигурността да са достъпни само за определени потребители със съответните потребителски права на достъп	Да	Да
2.5	Брой записи в регистъра на събития отнасящи се до сигурността	>1000 бр.	10000
2.6	Управление на сертификати - вградени и външни сертификати	Да	Да
2.7	Достъп до WEB сървъра чрез HTTPS	Да	Да
1.5	Сигурност при трансфер на файлове	Да	Да
2.8	Дистанционнен контрол на състоянието на устройството - SNMP (Trap&Get)	Да	Да
2.9	VPN - IPsec VPN	Да	Да
2.10	VPN– други типове поддържани от устройството	Да се посочи	Не се поддържа друг тип VPN
3	**Подържани протоколи**		
3.1	Secured IEC 60870-5-104, съгласно IEC 62351-3 TLS	Да	Да

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

08.2017

Документи 4.11.

Таблици 1, 2 и 3 в Приложение 9 от раздел I от документацията за участие - Изисквания към работата на RTU по стандарт IEC61850

ПРИЛОЖЕНИЕ 9

Таблица 1 – Основни изисквания

№	Описание	Изискване на ЕСО ЕАД	Предложение
1.	Предлаган модел	Да се посочи	RTU560
2.	Предлагана хардуерна и софтуерна версия	Да се посочи	Release 12
3.	Фирма – производител	Да се посочи	АББ АГ
4.	Държава, в която се произвежда	Да се посочи	Германия
5.	Поддръжка на IEC61850 Ed.1 с всички задължителни според стандарта функции	Да	Да
6.	Поддръжка на IEC61850 Ed.2 с всички задължителни според стандарта функции	Да	Да
7.	Възможност за едновременна работа на IEC61850 Ed.1 и Ed.2 в едно RTU	Да	Да
8.	Поддържа функция "Client" в Client/Server комуникации	Да	Да
9.	Поддържа функция "Server" в Client/Server комуникации	Да се посочи	Поддържа функция "Server" в Client/Server комуникации
10.	Поддържа функция "Publisher" в GOOSE комуникации	Да се посочи	Поддържа функция "Publisher" в GOOSE комуникации
11.	Поддържа функция "Subscriber" в GOOSE комуникации	Да се посочи	Поддържа функция "Subscriber" в GOOSE комуникации
12.	Поддържан SCSM	Използва IEC61850-8-1	Използва IEC61850-8-1

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

Таблица 2 – Изисквания към прилагането на протокол IEC61850

№	Описание	Минимално изискване на ЕСО ЕАД	Предложение
1.	Максимален брой IED в RTU по протокол IEC61850	≥ 80	120
2.	Максимален брой IED в един комуникационен интерфейс по протокол IEC61850	≥ 20	30
3.	Максимален поддържан брой "data set elements", които могат да се включат в един "data set"	≥ 200 "data set elements"	300 "data set elements"
4.	Какъв е максималният поддържан брой "data set elements", който може да се получават по IEC61850 – MMS	≥ 5000 "data set elements"	7000 "data set elements"
5.	Какъв е максималният поддържан брой "Report Control Blocks" (RCB)	≥ 800	1000
6.	Поддръжка на буферирани RCB (BRCB)	Да	Да
7.	Поддръжка на небуферирани RCB (URCB)	Да	Да
8.	Минимално множество поддържани „trigger conditions" на рапорта	• Data change • Quality change • Data update • General interrogation	• Data change • Quality change • Data update • General interrogation
9.	Поддържани "optional fields" на рапорта	Да се посочи	sequence-number; report-time-stamp; reason-for-inclusion; data-set-name; data-reference; buffer-overflow; entryID; conf-rev
10.	"Data set", включен в репорт може да се съставя от: • Structured Data objects • Data attributes	• Да • Да се посочи	• Да • Не се поддържат data attributes
11.	Минимално множество поддържани режими на управление	• Status only • Direct with normal security	• Status only • Direct with normal security

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

		• Direct with enhanced security • Sbo with enhanced security	• Direct with enhanced security • Sbo with enhanced security

АББ България ЕООД
Централен офис
бул. „Витоша" № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

Таблица 3 – Изисквания към съпровождащата документация, включена в предложенията на участниците

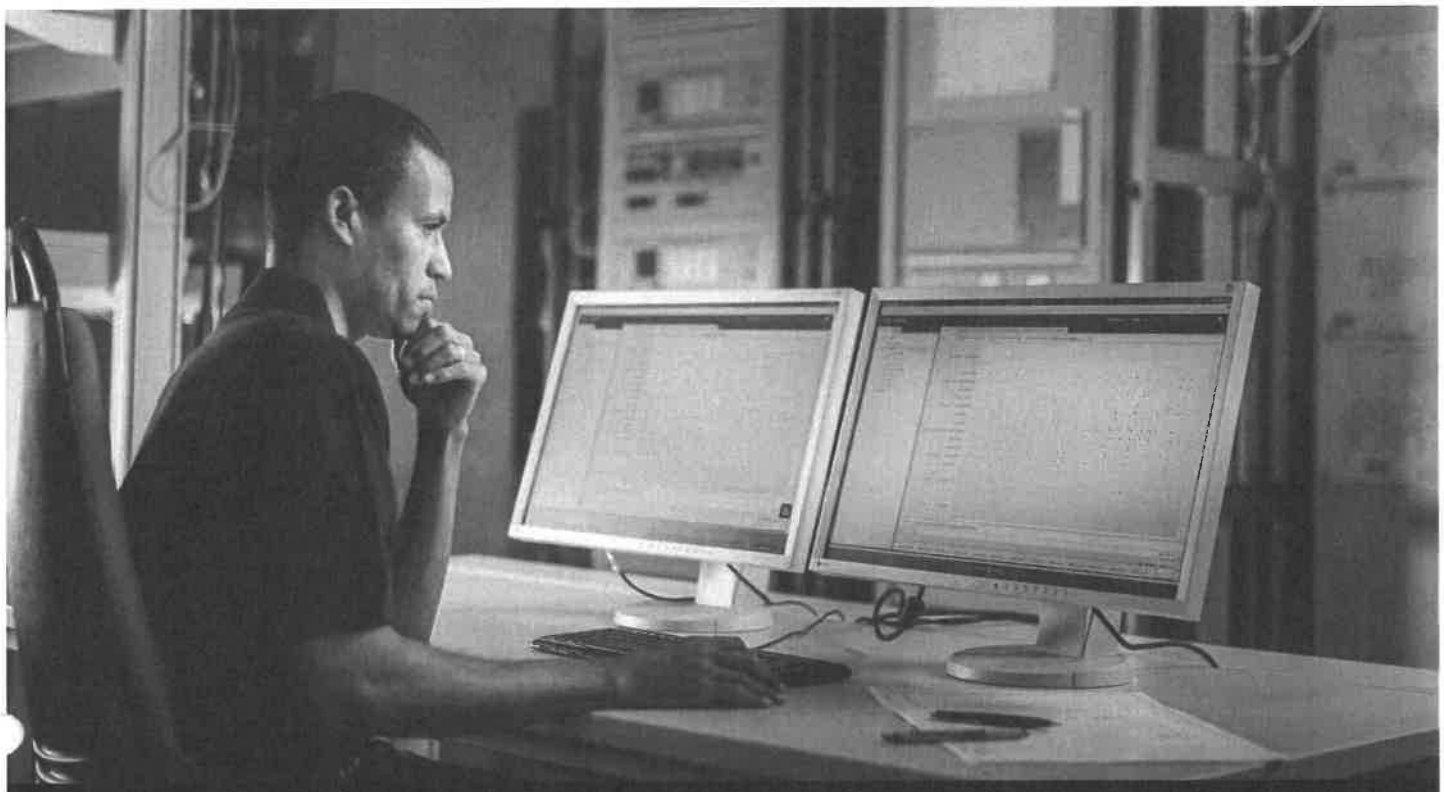
№	Описание	Изискване на ЕСО ЕАД	Предложение
1.	Да се представи декларация на производителя за съответствие „ACSI Basic Conformance Statement“	Да	Да
2.	Да се представи декларация на производителя за съответствие „ACSI Models Conformance Statement“	Да	Да
3.	Да се представи декларация на производителя за съответствие „ACSI Service Conformance Statement“	Да	Да
4.	Да се представи декларация на производителя за съответствие „Protocol Implementation Conformance Statement (PICS)“	Да	Да
5.	Да се представи декларация на производителя за съответствие „Model Implementation Conformance Statement (MICS)“	Да	Да
6.	Да се представи декларация на производителя “Protocol Implementation extra Information for Testing (PIXIT)“	Да	Да

АББ България ЕООД
Централен офис
бул. „Витоша“ № 89Б
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

Документ 4.15.

Параметри на комуникационния канал за дистанционно конфигуриране и тестване на RTU от работните станции и минималните изисквания за сигурност към този комуникационния канал.



System Data Manager SDM600
User Manual

Power and productivity
for a better world™

Contents

1 Copyrights

The information in this document is subject to change without notice and should not be construed as a commitment by ABB Oy. ABB Oy assumes no responsibility for any errors that may appear in this document.

In no event shall ABB Oy be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB Oy be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB Oy, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

Trademarks

ABB is a registered trademark of ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Guarantee

Please inquire about the terms of guarantee from your nearest ABB representative.

Third Party Copyright Notices

List of third Party Copyrights notices are documented in "about.htm" under the installation directory.

2 Introductions

2.1 Scope of the Document

This document is the user manual for the System Data Manager (SDM600) product. It provides information on SDM600, particularly on the available features and on how to engineer the system.

Depending on the purchased SDM600 license, some instructions in this document may not be relevant.

2.2 Use of symbols

This publication includes warning, caution and information symbols where appropriate to point out safety-related or other important information. It also includes tips to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:

Warning icon indicates the presence of a hazard which could result in personal injury.

Caution icon indicates important information or a warning related to the concept discussed in the text. It might indicate the presence of a hazard, which could result in corruption of software or damage to equipment/property.

Information icon alerts the reader to relevant factors and conditions.

Tip icon indicates advice on, for example, how to design a project or how to use a certain function.

Although warning hazards are related to personal injury, and caution hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, comply fully with all warnings and caution notices.

2.3 Abbreviations and Definitions

DR	Disturbance Record
FQDN	Fully Qualified Domain Name
GB	Gigabyte
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IP	Internet Protocol
kV	kilo Volt
LAN	Local Area Network
LN	Logical Node
PC	Personal Computer
RAM	Random Access Memory
RDRE	Logical node name for Disturbance Record
SA	Substation Automation
SCD	Substation Configuration Description
SDM	System Data Manager
SQL	Structured Query Language
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UI	User Interface
UNC	Universal Naming Convention
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSA	Vendor Specific Attribute
XML	Extended Markup Language

2.4 Related documents

- 1MRS757749 - SDM600 Installation Guide

- 1MRS757880 - SDM600 Release Notes

3 Safety information

This section has information on the prevention of hazards and taking backups from the system.

3.1 Backup copies

Taking backup copies

We recommend taking backup copies before making any changes, especially ones that might have side effects. Backup data needs to be copied to another place.

Backup copying makes it easier to restore the application software in case of disk crash or other severe failure where stored data is lost. It is therefore recommended that backup copies are taken regularly.

General best practices for backing up system is to have at least two backup copies. A new backup is copied over the oldest backup. This way the latest version is always available, even if the backup procedure fails.

Detailed information on how to make a backup is available in the user manual.

3.2 Fatal errors

A fatal error is an error that causes a breakdown or a locked situation in the SDM600 program execution.

Handling

In case of a fatal error:

1. Write down the possible error messages
2. Copy the folder Log under SDM600 installation directory
3. Open Event Viewer and look for SDM600 errors under WindowsLogs Application folder
4. Restart the PC where SDM600 is installed

Avoid shutting down the PC by powering off the PC directly as this may cause damage on the base system file.

Report the program break-down together with the possible SDM600 error messages and the log files under the log directory to your SDM600 representative.

4 Product overview

SDM600 – we see the unseen from a different perspective

The primary business of any utility is delivering services to their customers, and they have the tools and techniques to ensure contiguous delivery. But as those tools multiply the incoming data becomes unmanageable, while the complexity of tracking IED software versions and user accounts risks undermining the advantages that system automation brings. To manage the management network requires a new toolset, to see the unseen, protect the unguarded, and master the unwieldy.

SDM600 sees the unseen: with full support for IEC61850 interfaces, and the capability to talk to legacy equipment, it interrogates IEDs around the network. From those IEDs it gathers disturbance recorder files and collates them for centralized storage. SDM600 then analyzes the incoming data and produces concise reports so utilities can see patterns of activity, or identify correlations in performance, by seeing what had previously been hidden.

The centralized storage of disturbance files enables them to be extracted with ease, enabling the data to be shared with analysis software or aggregated with data from the rest of the grid to create a holistic view of operations.

SDM600 protects the unguarded, by creating a single point of management for user accounts and access control, and logging security events affecting the network. Cybersecurity is a vital component in modern networks, but access policies fragmented across network devices risk exposing critical vulnerabilities. The dispersed nature of automation networks has complicated tasks such as revoking staff credentials, or removing default passwords, but SDM600 brings back the simplicity by providing a single place in which accounts can be managed and access controlled: a gatekeeper to the automation network.

SDM600 masters the unwieldy, checking up on IEDs to ensure they are running the latest software, have the latest patches installed, and are properly configured for the tasks assigned to them. The complexity of modern software demands it become a changeable thing, constantly updated in response to new security concerns, or functionality fixes, or to add new features. IEDs are no exception to this, and keeping track of software versions can become significantly onerous without a management system such as SDM600 to take care of it.

Information is only as good as the way in which it's displayed, and with a web-based interface SDM600 creates a unique visualization of the automation network and the IEDs of which it is comprised. Security events, disturbance reports, and IED software versions are all collated into a single dashboard from which the user can share the insight of the SDM600, and see the unseen from a different perspective.

5 Accessing SDM600

SDM600 is a client server based Rich Internet Application solution. To use SDM600, a web browser is needed.

A Rich Internet application (RIA) is a web application that has many of the characteristics of desktop application software. For more information on RIA, see *http://en.wikipedia.org/wiki/Rich_Internet_application*.

5.1 Secure Connections

SDM600 can only be accessed by using an HTTPS connection (secure connection). A secure connection means a connection that is established by a combination of two protocols, namely HTTP and TLS. TLS are cryptographic protocols that provide security in network connections.

To establish a secure connection, on the first connection to the SDM600 server, your browser may issue a warning about the validity of the certificate that is used for encrypting the connection. The warning is issued because SDM600 uses a self-signed certificate. A self-signed certificate is an identity certificate that is signed by the same entity that issues the certificate. In this particular case, during the installation, SDM600 issues a self-signed certificate to establish TLS communication between the client and the server.

5.2 Security certificate warnings

If a browser is not able to verify the certificate that is used to established the secure connection to the SDM600 server, a warning is shown. This is because SDM600 comes with a self-signed certificate. To obtain a certificate that is signed by a well-known certification authority, such as VeriSign or Thawte, each organization that installs SDM600 has to order this directly from the respected certification authority website as organization-specific information is needed to obtain the certificate. If there is a well-known certification authority signed TLS certificate available, install it on the server where SDM600 is installed. For more information, please consult your IT administrator.

In addition, if it is not possible to obtain a certificate from a proper or well-known certification authority, it is also possible to configure the PC that accesses SDM600 to trust SDM600. This can be done by installing ABB SDM600 certificates from User Application and Settings, Download tab.

Security certificate warning in Microsoft Internet Explorer

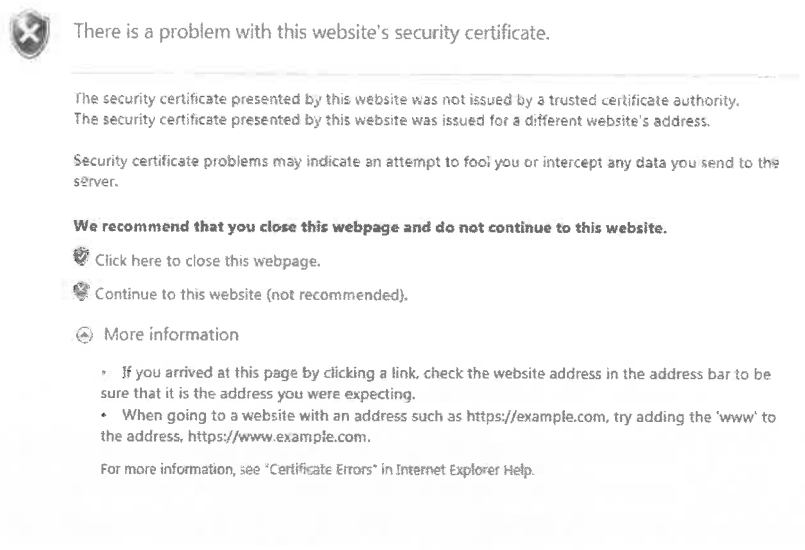


Figure 5.1: SDM600 Site Access - Warning on Security Certificate Issue - Internet Explorer Browser

When this warning is shown, click **Continue to this website (not recommended)**. The SDM600 login page opens.

Security certificate warning in Mozilla Firefox

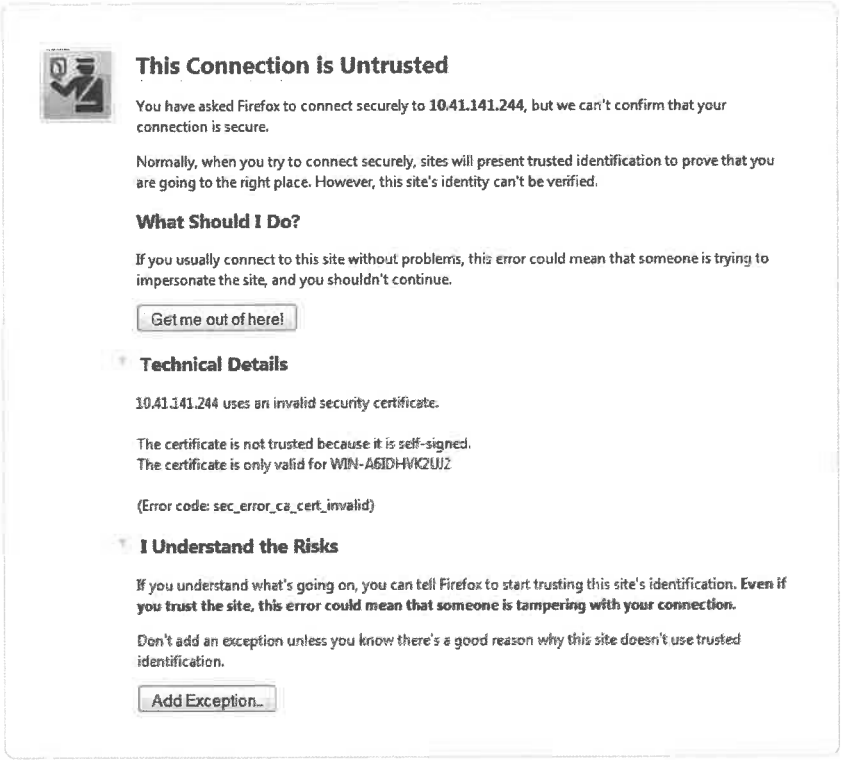


Figure 5.2: SDM600 Site Access - Warning on Security Certificate Issue - Mozilla Firefox Browser

When this warning is shown, click **Add Exception**. A window opens where an exception to this particular page can be added:

Figure 5.3: SDM600 Site Access - Add Exception to the SDM600 Site - Mozilla Firefox Browser

To proceed, click **Confirm Security Exception**. The SDM600 login page opens.

Protected Mode in Microsoft Internet Explorer

Microsoft Internet Explorer comes with an additional feature called Protected Mode. When this feature is activated, Microsoft Internet Explorer makes it more difficult to install malicious software on your computer. However, this also blocks several features that are introduced in SDM600. To overcome this and still protect your computer from malicious software, there are two ways: disabling the Protected Mode feature for the local intranet only or running the browser as administrator.

To disable the Protected Mode feature only for the local intranet, do the following:

1. Select **Control Panel > Internet Options**, and open the **Security** tab.
2. Click **Local Intranet**, then uncheck the **Enable Protected Mode** option.

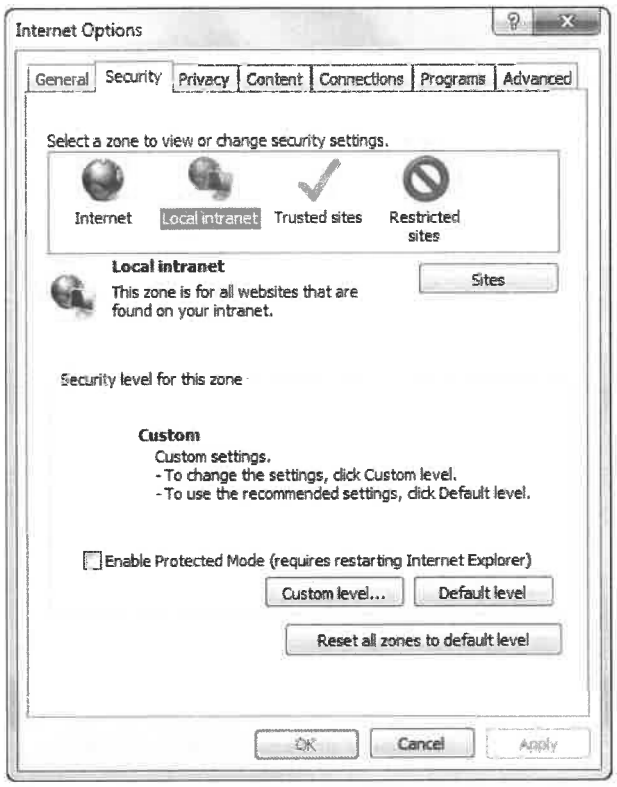


Figure 5.4: Disabling Protected Mode - Microsoft Internet Explorer Browser

3. To customize the list of your intranet site, in the same window, click **Sites**. A new window opens. Click **Advanced**.

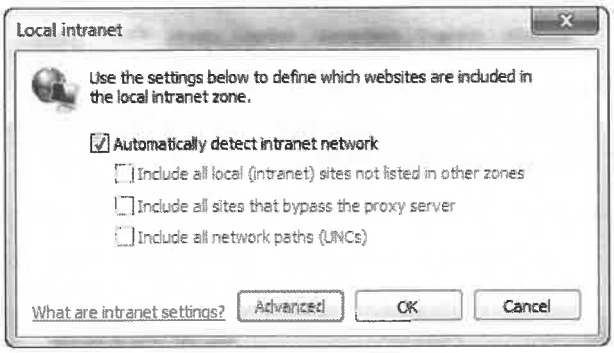


Figure 5.5: Disabling Protected Mode - Microsoft Internet Explorer Browser - Add Custom Site to Intranet Network Definition

4. In the following window, add the address of SDM600, then click **Add**. After that, click **Close**. To close all the remaining windows, click **OK** in each window.

Figure 5.6: Disabling Protected Mode - Microsoft Internet Explorer Browser - Add IP Address of SDM600

5. Restart the Microsoft Internet Explorer browser.

It is not recommended to disable the Protected Mode feature for Internet Explorer. This certainly increases the possibility that your PC will be infected by malicious software. If your SDM600 is designed to access through a wide internet connection, it is recommended to set up a VPN connection. Setting up a VPN connection is not in the scope of this guide.

For more information on the Protected Mode feature in Microsoft Internet Explorer, see *http://windows.microsoft.com/ en-gb/windows-vista/ what-does-internet-explorer-protected-mode-do*.

To start your browser as an administrator, do the following:

1. Select **Microsoft Windows Start menu > Internet Explorer**.
2. Press the right button of the mouse, then select **Run as administrator**.

5.3 Network Configuration

SDM600 can be accessed remotely via a network or locally from the installed computer. To access SDM600 over the network, some specific network settings are required. Particularly when the computer that is used to access SDM600 is in the same subnet as the SDM600 server and firewall rules allow access to the SDM600 server. Nonetheless, the following settings are provided as a general guideline.

5.3.1 IP Address

SDM600 is a server product that comes with different features. It is important to assign a static IP address to the PC where SDM600 is installed.

The static IP address is used for accessing SDM600 as well as for user authentication, centralized activity logging and other core SDM600 functionality. Failing to assign a static IP address may result in a non-operational SDM600.

Furthermore, as SDM600 is accessed by multiple systems, applications, and devices in the substation automation system, it is important to ensure that SDM600 can be reached from the systems, applications, and devices that need the SDM600 service. In the same way, it is important to ensure that SDM600 is able to reach the IEDs in the substation for disturbance records collecting purpose.

For information on your system network design and on how to integrate SDM600 into the network infrastructure, please consult with your network administrator.

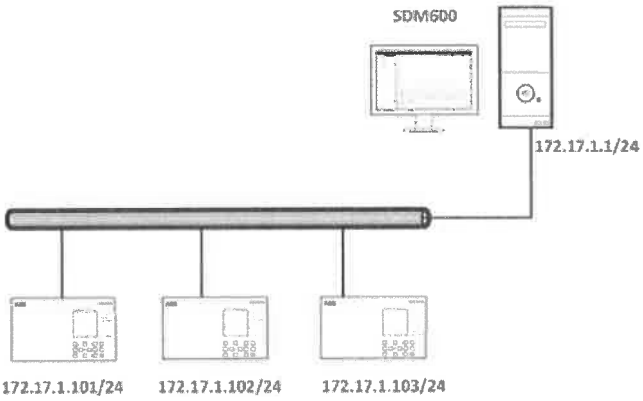


Figure 5.7: An example of a network setting for theSDM600 system

The SDM600 server in a substation should be in the same network as the IEDs in order to be able to connect them.

5.3.2 Virtual LAN (VLAN)

If the automation network is configured or segmented using Virtual LAN (VLAN), it needs to be ensured that the VLAN traffic that comes and goes out of SDM600 is properly configured.

It is recommended that the respective network administrator is always involved while deploying SDM600 in your organization.

5.3.3 Firewall

Hardware and software firewalls can block traffic from or to SDM600. To function properly, SDM600 requires the following default ports to be opened:

Port No.	Purpose
389 TCP	Port for SDM600 Centralized Account Management (LDAP Authentication)
443 TCP	Port for HTTPS web access
636 TCP	Port for SDM600 Centralized Account Management secure connection (LDAP Authentication)
1433 TCP	Port for SQL Server
1468 TCP	Port for SDM600 Centralized Activity Logging Service (Syslog over TCP)
1812 UDP and TCP	Port for SDM600 Centralized Account Management Service (RADIUS communication)
58900 TCP	Port for SQL Server
59100 - 59199 TCP	SDM600 internal service (Parent-Child Initialization)
59200 TCP	SDM600 internal service (Centralized Activity Logging Service)
59990 - 59999 TCP	SDM600 internal service (Parent - Child, Hot-Standby Initialization)
60000 - 60010 TCP	SDM600 internal service (Hot - Standby)
61743 TCP	SDM600 internal service - open only during migration from previous versions of SDM600
514 UDP	Port for SDM600 Centralized Activity Logging Service (Syslog over UDP)

Each firewall device / software comes with an instruction manual on how to configure the firewall to allow certain traffic to pass.

It is not recommended to disable any firewall without first informing the network administrator in your organization. The firewall should only be disabled during testing sessions.

In general, while setting up the SDM600 Parent-Child relationship and if you have your operating system firewall

enabled, it is important that all the listed ports are excluded from the firewall rules.

5.3.4 Power Management

To ensure that the operation of SDM600 is not interrupted by the power optimization behavior, the power management function can be modified so that the power profile is set to high performance.

While setting the computer power profile to high performance, it is important to set the computer to never go to sleep mode. Or you can also set the monitor to never turn off.

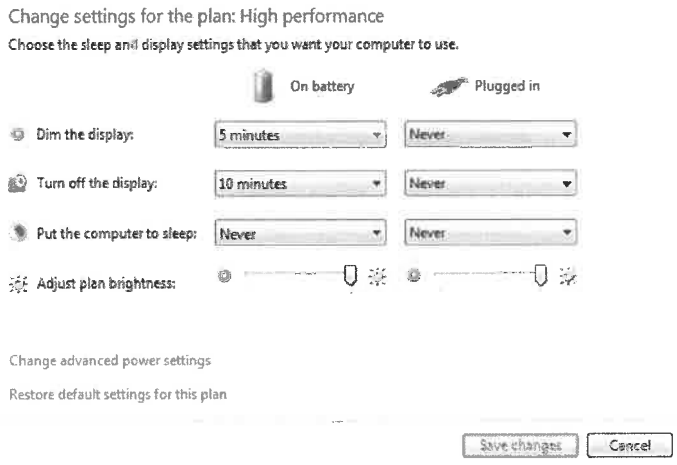


Figure 5.8: Power management settings in Windows 7 x64 Operating System

5.4 Login into SDM600

SDM600 provides a login page to get into SDM600. When a user load the SDM600 on a browser or after logout from SDM600, a login page is shown. To login into SDM600, a user has to enter a valid credentials (username and password). After entering the valid credentials, the user will be offered to select a single role (if the user is assigned to more than one roles) which the user wants to use to login into the SDM600. Best practices in cyber security recommend the principle of least privilege. Therefore, if a user has more than one roles, it is important to remember that the user should login only with role that fits to the tasks that are going to be done at that login session. When the user has only one role assigned, SDM600 will immediately log the user into SDM600 if the entered

credentials are valid. Information regarding user management can be found in the Section about Centralized Account Management.

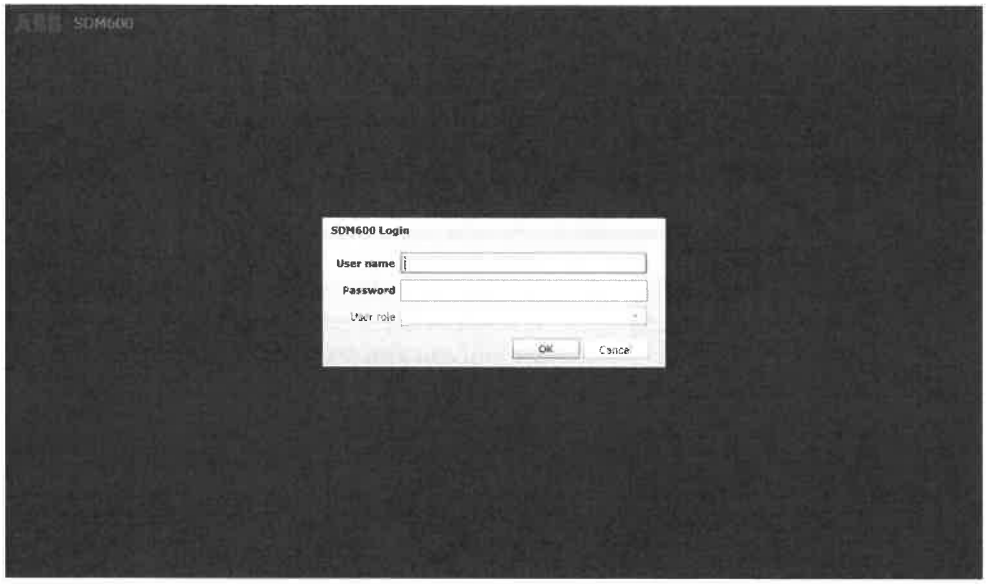


Figure 5.9: SDM600 Login Page

6 Navigation in SDM600

The SDM600 user interface (UI) is based on the Microsoft Silverlight technology. It is a web-based UI and designed to be easily used and navigated.

The SDM600 content is automatically updated when there is a new update available. Therefore, unlike a normal website where the content can be refreshed by pressing the F5 key, in SDM600, pressing the F5 key reloads the overall SDM600 application and subsequently a user will be reauthenticated.

The SDM600 UI is divided into four main areas:

- Navigation reference area (indicated with an orange box in the following figure)
- Content specific area (indicated with a red box in the following figure)
- User information and application settings area (indicated with a green box in the following figure)
- Toolbar area (indicated with a blue box in the following figure)

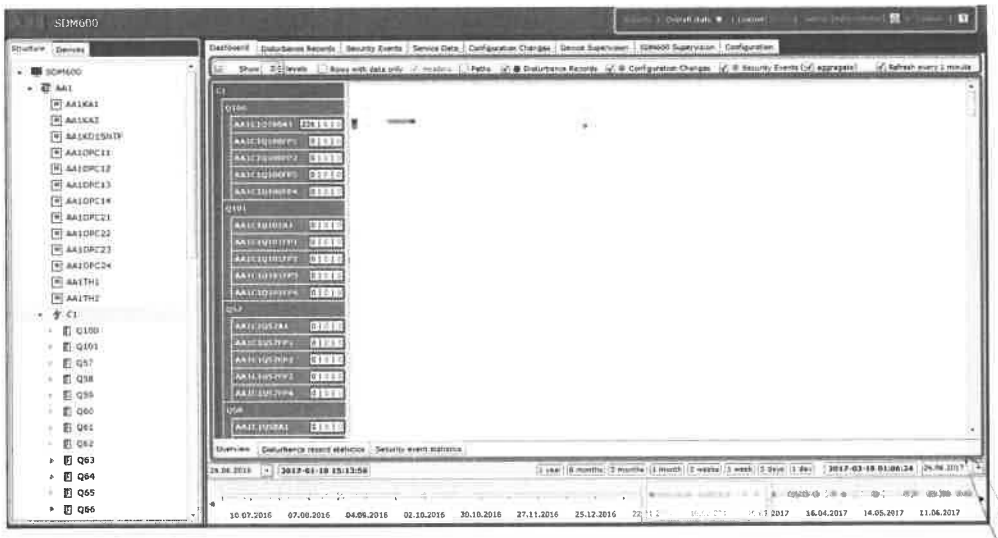


Figure 6.1: Areas in the SDM600 UI

6.1 Navigation reference area

The left panel of the SDM600 UI is called the *navigation reference area*. This area helps the user to explore the system that is monitored or managed by SDM600. A selected entity in this panel automatically becomes a filter for the information shown in the right panel of the UI.

There are two tabs in the navigation reference area:

- The *Structure tab* shows the structure of the configured substation and the connected SDM600 devices.
- The *Devices tab* shows the available devices that are directly connected to the installed SDM600.

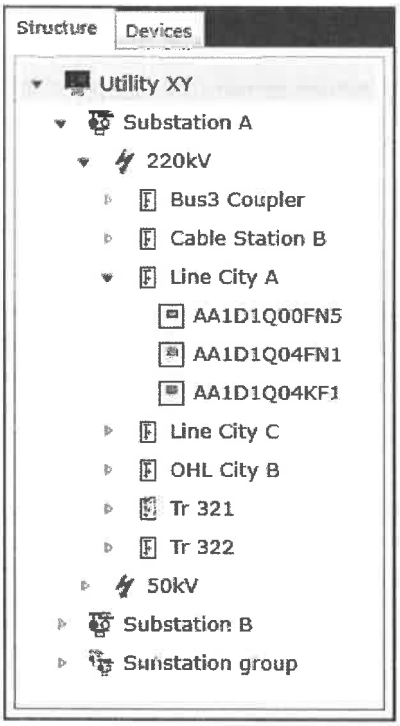


Figure 6.2: SDM600 Navigation Reference Area - Structure tab

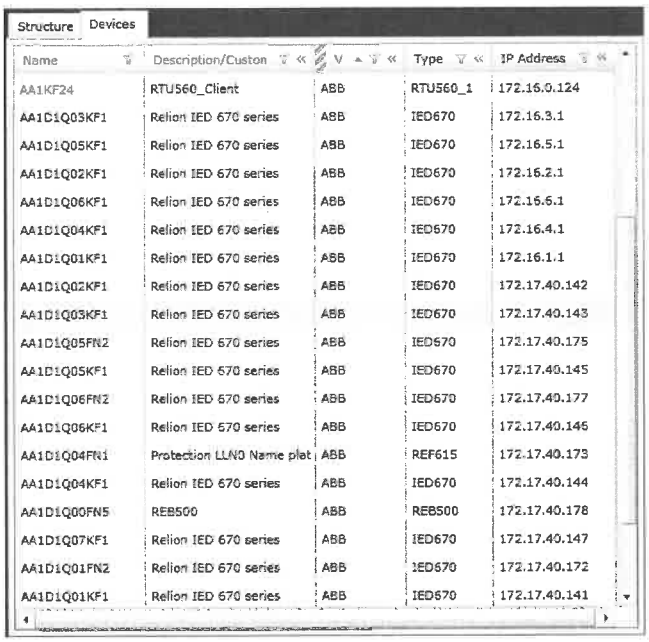


Figure 6.3: SDM600 Navigation Reference Area - Devices tab

6.2 Content Specific Area

The right panel in the SDM600 UI is called the *content Specific area*. This area is divided into four sub-application areas:

- The *Dashboard tab* shows information of the system under observation in a two-dimensional graphical format.
- *Application area tabs*. Each application in SDM600 has a dedicated tab. The current version of SDM600 has the Disturbance Records, Security Events, Service Data, Configuration Changes, Supervision and Configuration tabs available.
- The *Device supervision tab* shows a list of the connected devices and their status.
- The *SDM600 Supervision tab* shows the operational status of SDM600.
- The *Configuration tab* contains multiple subtabs that are used for configuring SDM600.

SDM600 Dashboard Tab

The SDM600 Dashboard tab presents graphical information of the system under observation. The system can be a substation, a group of IEDs or substations, or another SDM600 device. The Dashboard tab contains three sub-tabs: the two-dimensional points-graph tab, a bar chart graph to show the statistics of the collected disturbance record entries, and a spider-web graph to show the statistics of the collected cyber security events in the system.

Figure 6.4: SDM600 Application Context Area - Dashboard Tab

SDM600 Tabs for Application Area

These tabs are a collection of application-related tabs. The Disturbance Records, Security Events, Service Data, Configuration Changes, Supervision and Configuration tabs are available. The Disturbance Records tab shows the collected disturbance records and presents them in a grid view. The Security Events tab shows the collected security events (in Syslog (RFC 5424) format) that are received by SDM600 from the connected systems, applications, or devices. The Configuration Changes tab shows the collected changes in the device's configuration and presents them in a grid view.

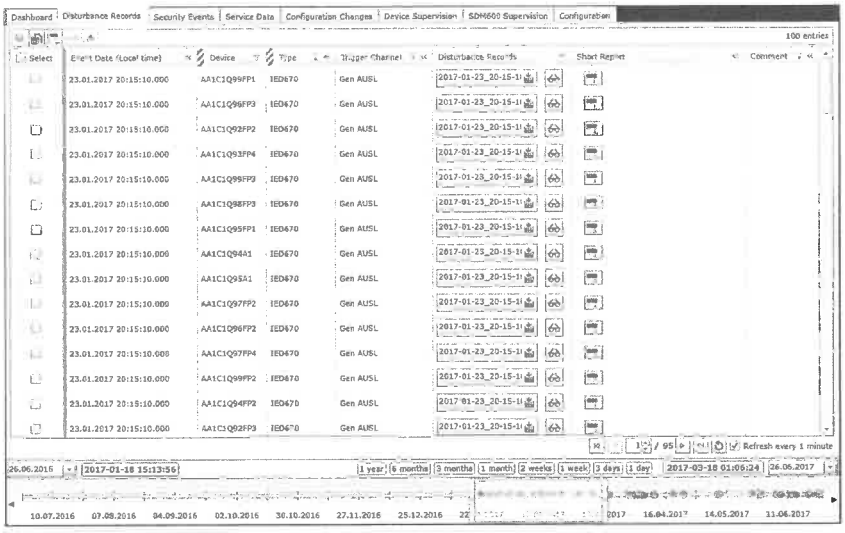


Figure 6.5: SDM600 Application Context Area - Disturbance Records Tab

SDM600 Service Data Tab

The Service Data tab shows information useful for managing installed base like:

- *Device name* - shows name of the device. If native or web based configuration tool is set, then *Device name* is a link, which is opening configured tool.
- *Type* - shows type of the device.
- *Serial Number* - shows serial number of the device.
- *Configuration version* - shows version of the configuration running on the device.
- *Software version* - shows version of the firmware installed on the device.
- *Details* - open another window with protocol specific details.
- *Patches* - open another window with list of installed patches. This option is available for Windows Client only.
- *Configuration* - if configuration file for the device is stored in SDM600, then link to download of configuration to the disk is activated.
- *Firmware* - this checkbox is checked if there is firmware stored in SDM600 for the particular device.

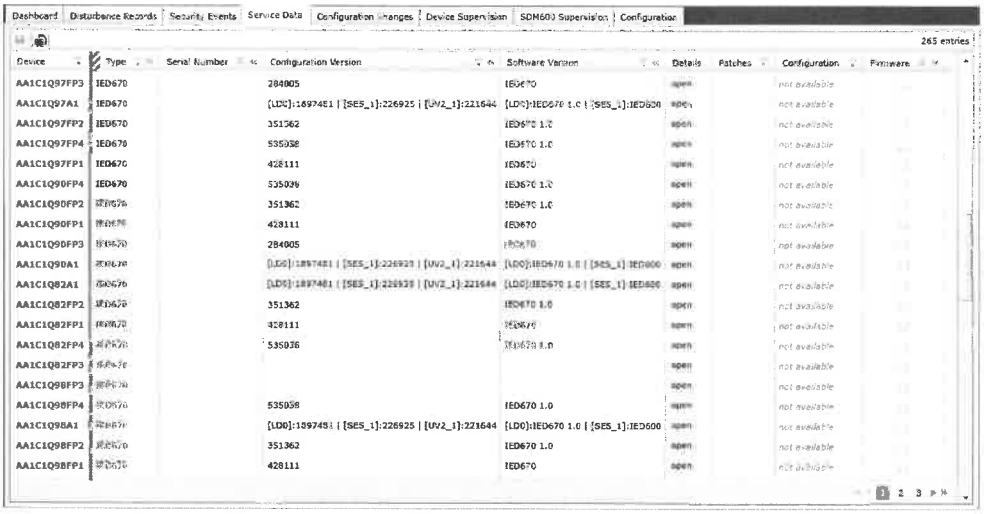


Figure 6.6: SDM600 Service Data Tab

SDM600 Supervision Tabs

The Device Supervision Tab shows a list of the devices that are managed by SDM600, for example, IEDs, computers, network devices and connected SDM600 devices. The Device Overview Tab shows the following details regarding a device:

- *Name*: the name of the device. If IP address or configuration tool of the device is set, (refer to the *Setting Up the IEDs/Devices* chapter) then *Name* is a link which is opening device's web page or configured tool.
- *Connection status*: the reachability status of the device (by means of the last access)
  - *Unknown*: IP address of the device is not configured, or status has not been checked.
  - *Red*: the device is unreachable or sends no feedback.
  - *Yellow*: the device is reachable, but there are problems with communication.
  - *Green* : connection is working correctly
  - *No license*: Disturbance records retrieval is configured, but SDM600 device is not licensed to retrive DRs from this device.
- *Time of last status change*: the time of the last status change.
- *DR Operation warning*: a warning about a problem detected in connection status. The following warnings are available: *No MMS protocol*, *Invalid DR Path*, *No FTP protocol*,*NMMS library can't connect with: <IP address>*, *Unable to Ping device*, and *Invalid User name and password*.
- *Type:* the type of the device.
- *Description /Custom Name:*
- *NERC-CIP Rating:* Possible values are: Not Applicable, Low Impact, Medium Impact, High Impact
- *IP address*: the IP address of the device.
-

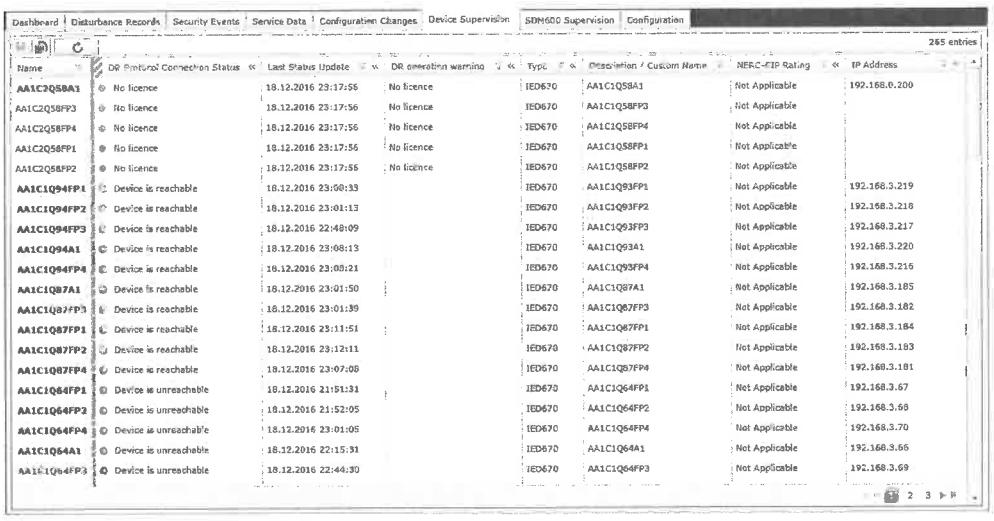


Figure 6.7: SDM600 Device Supervision Tab

The SDM600 Supervision tab shows information and status of the SDM600 . Tab is divided in to five sections:

- *General* - shows general status of the SDM600, version number and all IP addresses recognized by SDM600
- *Services* - shows status of SDM600 services
- *Database* - shows path to Database folder and size of SDM600 databases

Microsoft SQL Express has limitation to 10Gb per database file. When your database size is reaching this limit, consider to upgrade database engine to Microsoft SQL Server Standard.

- *License* - shows licensing information and number of used licenses vs. all licenses available for particular feature.

Figure 6.8: SDM600 Supervision Tab

SDM600 Configuration Tab

The Configuration Tab contains several subtabs that are needed to configure SDM600:

- General Settings tab
- Tabs for configuring SDM600: Structure, Hierarchy, Device Settings
- Tabs for user management in SDM600: Centralized Account Management, User Management, SDM600 User Rights
- E-mail Notification tab
- Application-related configuration tabs: Disturbance Record Retrieval, Security Events, Event Mapping and File management
- SDM600 maintenance tab: Backup & Restore tab

Figure 6.9: SDM600 Configuration Tab

SDM600 Service Data Tab

The Service Data Tab shows the following details regarding a device:

- *Device name* - shows name of the device. If native or web based configuration tool is set, then *Device name* is a link, which is opening configured tool.
- *Type* - shows type of the device.
- *Serial Number* - shows serial number of the device.
- *Configuration version* - shows version of the configuration running on the device.
- *Software version* - shows version of the firmware installed on the device.
- *Details* - open another window with protocol specific details.
- *Patches* - open another window with list of installed patches. This option is available for Windows Client only.
- *Configuration* - if configuration file for the device is stored in SDM600, then link to download of configuration to the disk is activated.
- *Firmware* - this checkbox is checked if there is firmware stored in SDM600 for the particular device.

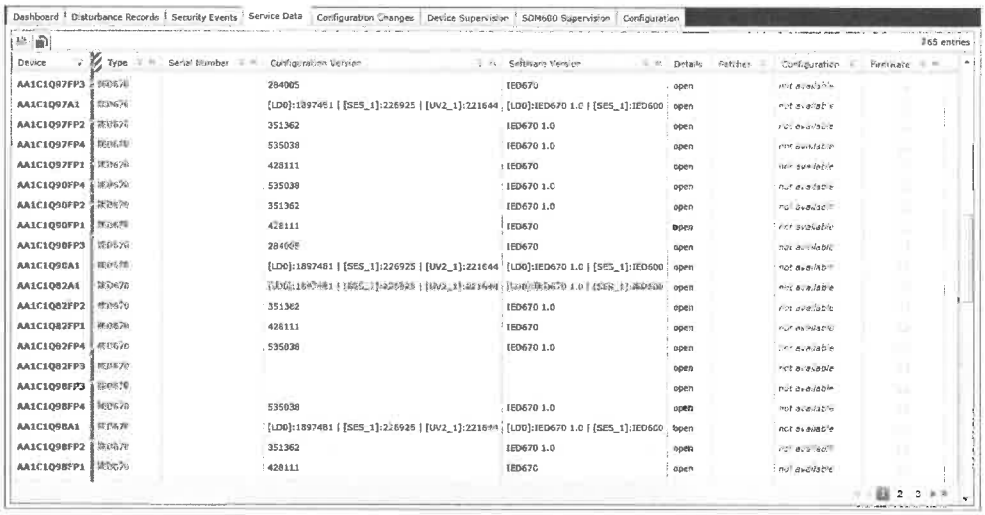


Figure 6.10: SDM600 Service Data Tab

6.3 Toolbar Area

At the top of the right panel of SDM600, there is a toolbar that provides several common functionalities, such as exporting a grid table into the Microsoft Excel format or saving the updated configuration. There are also some context-specific functionalities, for example, short report generation is only available when the Disturbance Records tab is highlighted.

In the right end of the toolbar, the number of entries in the highlighted tab is shown.

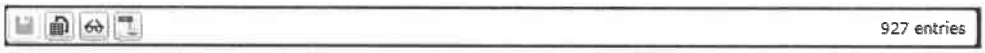


Figure 6.11: SDM600 Toolbar Area from Disturbance Records Tab

6.4 User Information and Application Settings Area

In the top right corner of the SDM600 UI, the following information is shown:

- *Reports*: Opens a window with reports generated on the server. Reports are stored in the servers for 1 hour.

- *Overall state*: the overall operational state of SDM600. State dot can be red or green. Whenever there is an issue with a core component of SDM600, this indicator turns red.
  There are two indicator types:
  - single dot for standalone configuration

  - double dot for hot-standby configuration

  When SDM600 is connected in hot-standby relation, then left dot is showing status of local system and right dot is showing status of remote partner.

- *License*: the type of license used by SDM600. It can be a demo license or, if a proper license is used, the license information is shown as *Valid*.
- *User name*: the username that is used to log in to SDM600.
- *Current user role*: the role that is used to log in to SDM600.
- *Settings*: a link to the settings where users can modify their user information, modify application settings, or download some required software.
- *Logout*: this will log the current user out of SDM600.
- *Help*: a link to the help function and to *About SDM600*.

Figure 6.12: SDM600 User Information and Application Settings Area

When clicking the help button, two options are shown:

- Help option: opens the SDM600 User Manual

When the Help option is clicked, the SDM600 User Manual is opened in a new pop-up window. In some browsers, the pop-up blocker feature is enabled by default which causes the user manual window not to open. To open the user manual, first disable the pop-up blocker for your browser.

The SDM600 User Manual can also be found under the *UserManuals* folder of the SDM600 installation folder,

by default, this folder is under *C:\Program Files (x86)\ABB\SDM600\UserManuals*.

- About option: opens an SDM600 About box

Figure 6.13: SDM600 About box

7 SDM600 Dashboard

The SDM600 Dashboard has two parts:

- SDM600 Overall Status Dashboard
- SDM600 Application-Specific Dashboard

SDM600 Overall Status

The SDM600 Dashboard UI is a two-dimensional plot area. It shows three types of events from the system under observation, based on the entity that is selected on the SDM600 Navigation Reference Area. The event types are:

- Disturbance record events - represented by blue dots
- Device configuration change events - represented by green dots
- Security events - represented by orange dots

The X axis of the dashboard represents the time of an event and the Y axis represents the location where this particular event happens.

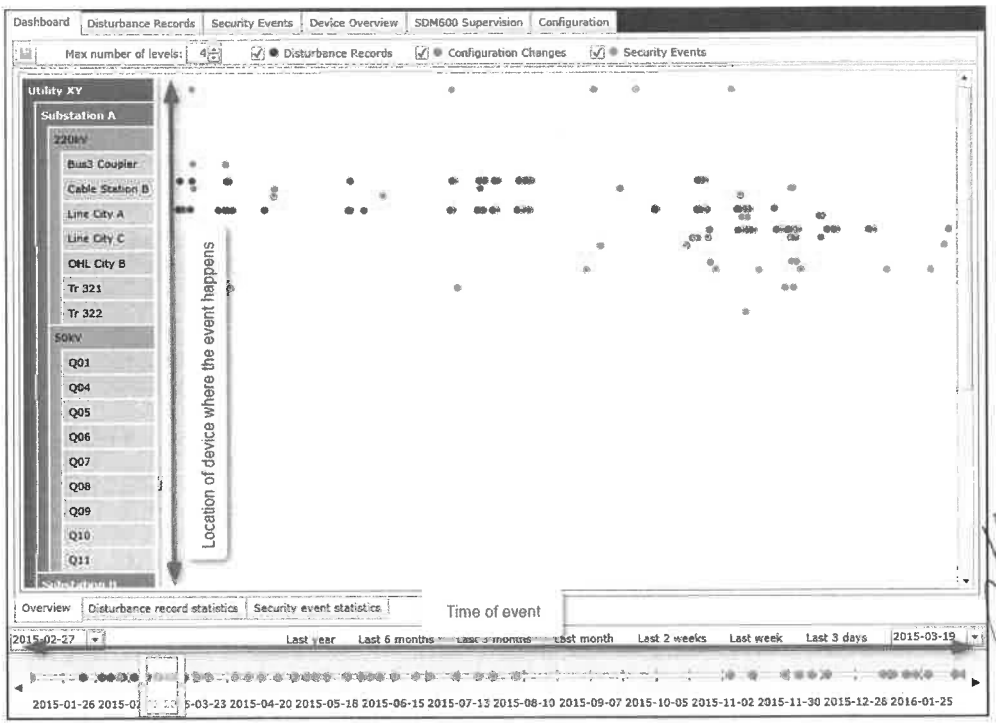


Figure 7.1: SDM600 Dashboard

The dashboard UI can show a wide range of data. It has a Zoombar Time Navigator for navigating the dashboard. To zoom into a specific date range, click the Zoombar control and move the mouse to the intended date limit, then release the mouse. Do this for both

ends. To move to another date range, click the Zoombar Time Navigator, then move and release the mouse.

Figure 7.2: SDM600 Dashboard Zoombar Time Navigator

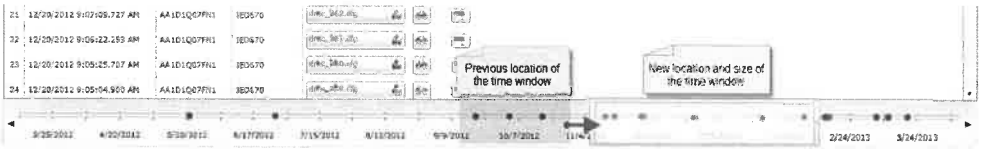


Figure 7.3: SDM600 Dashboard Zoombar Time Navigator Shifted

Each dot in the dashboard can be clicked. When hovering over a particular point, a tooltip box shows information relevant for that point.

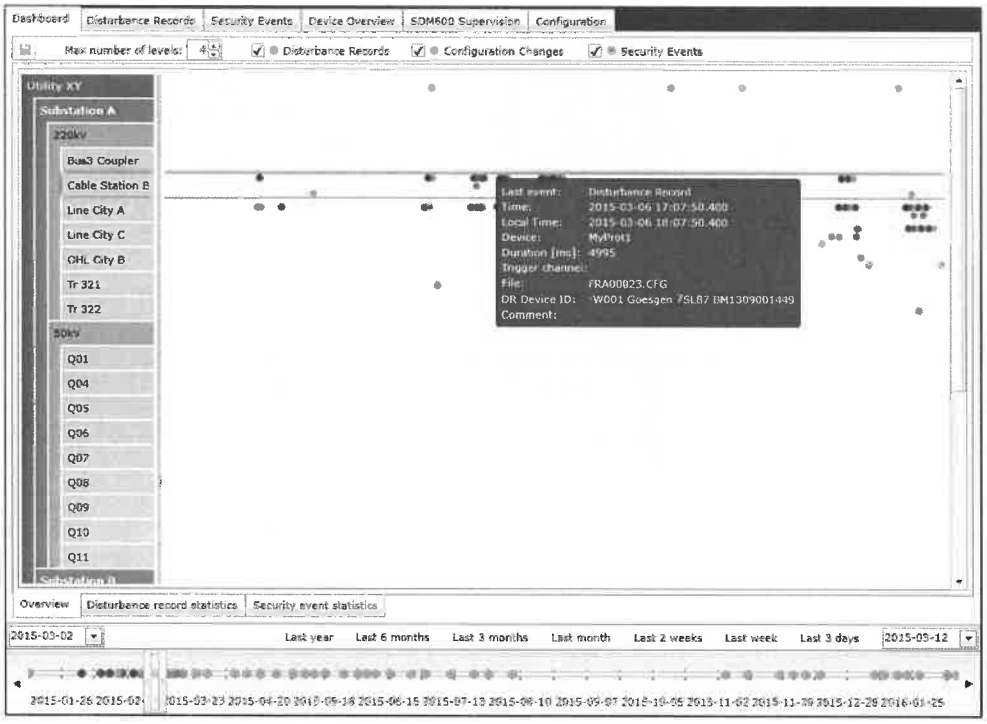


Figure 7.4: SDM600 Dashboard - A Click on A Dot

When clicking a disturbance record event (blue dot), a security event (orange dot) or a device configuration change events (green dots), SDM600 automatically navigates to the Disturbance Records tab, Security Events tab or Configuration Changes tab respectively. In addition, the record in focus is highlighted.

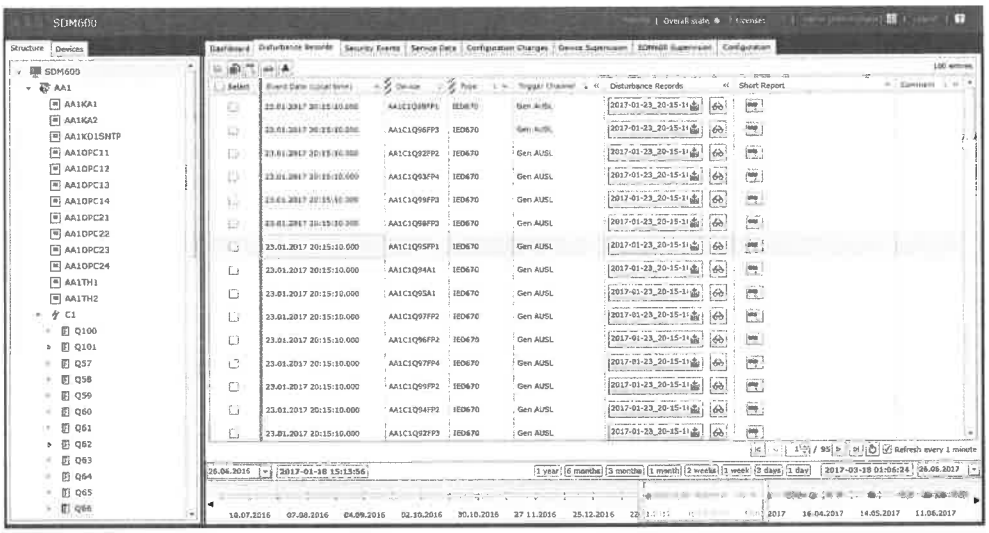


Figure 7.5: SDM600 DR Entry Highlighted from Dashboard Point

When right-clicking a Disturbance record event (blue dot), two context menus are shown:

- *Evaluate*: opens a tool to launch and analyze the disturbance record event
- *Short Report*: generates a short report of the disturbance record event

Figure 7.6: SDM600 toolbar area on the dashboard

SDM600 allows to configure how many levels of the structure tree will be visible on the dashboard. Number of tree levels can be defined in the toolbar area in the dashboard.

Option *Rows with data only* is presenting rows from devices where Disturbance Records, Configuration Changes or Security events are stored in SDM600. This option is reducing number of displayed lines.

Option *Paths* is adding full path to the device name.

There is also possibility to filter information presented on the dashboard. By default Disturbance Records, Configuration Changes and Security Events are selected. For large number of security events generated in the short amount of time there is possibility to aggregate security events entries. When this checkbox is selected then all security events form single day are represented by one dot on the dashboard.

Button with an arrow (indicated by red box on the following figure) is refreshing dashboard on demand.

Figure 7.7: Dashboard refresh button

If there is a large number of information to display on the dashboard, then it's recommended to uncheck "*Refresh every 1 minute*" option and select *aggregate security events*.

This will prevent form automatic dashboard refreshing, decrease amount of dots to render and increase performance.

SDM600 Disturbance Record Statistics

The Disturbance record statistics tab shows a bar chart of the disturbance record events in the entities that have been selected in the Navigation Reference Area.

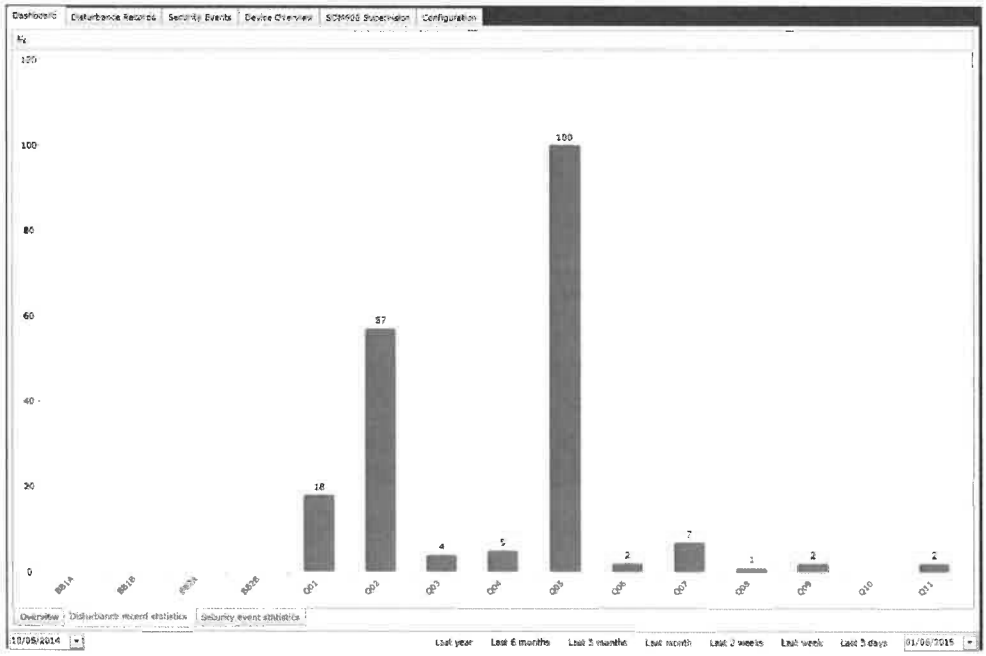


Figure 7.8: SDM600 DR Specific Dashboard

SDM600 Security Event Statistics

The Security event statistics tab shows a radar chart of the recorded security events in SDM600 based on the selected entities in the Navigation Reference Area. The radar

chart has security event categories as its axes. SDM600 provides the following security event categories:

- *Security – accountability*: any events from a user, which ensures unique traceability to that particular user. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
- *Security – administration and configuration*: any events that come from administering or configuring cyber security measures in the system
- *Security – potential security violation*: any events that may come from potential security violation actions
- *Security – operation*: any operational events from cyber security measures
- *System – engineering and configuration*: any events that come from engineering and configuration of industrial control systems
- *System – operation*: any events that come from operational of industrial control systems
- *System – maintenance*: any events that come from maintenance activitity on industrial control systems
- *System – monitoring*: any events that come from monitoring the operational of industrial control systems
- *Communication*: any events that relate with the establishment, operation, or de-establishment of communication-related functions or devices in industrial control systems
- *Unknown*: any uncategorized or unknown events or or any events that cannot be interpreted by the existing interpreter engine.

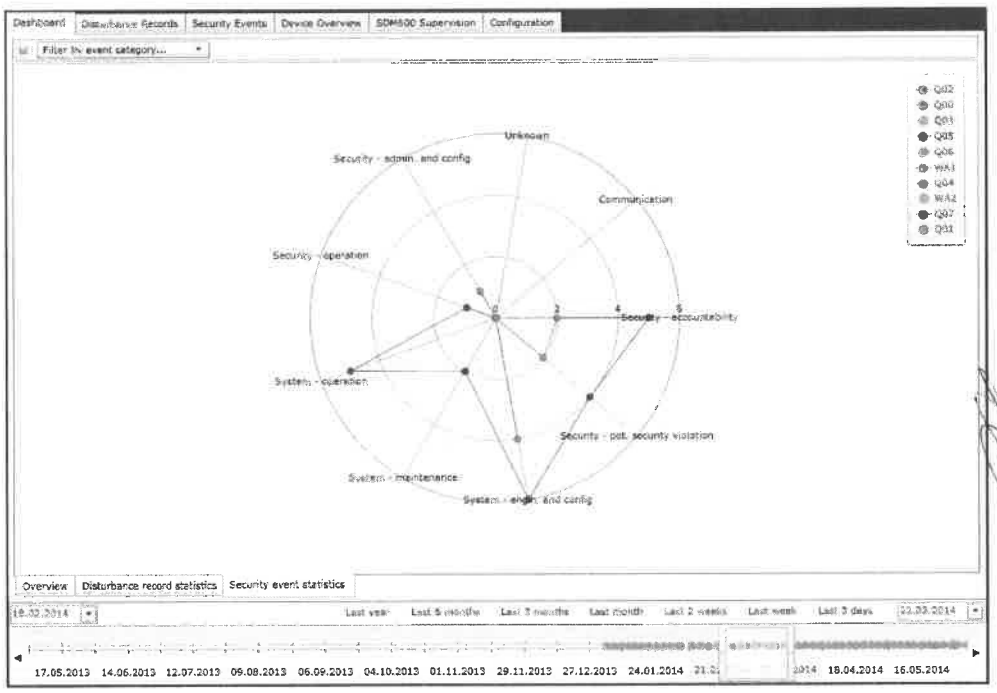


Figure 7.9: SDM600 Security Event Statistics

8 Configuration of SDM600

8.1 General Settings

General Settings is the first subtab of the Configuration Tab in SDM600.

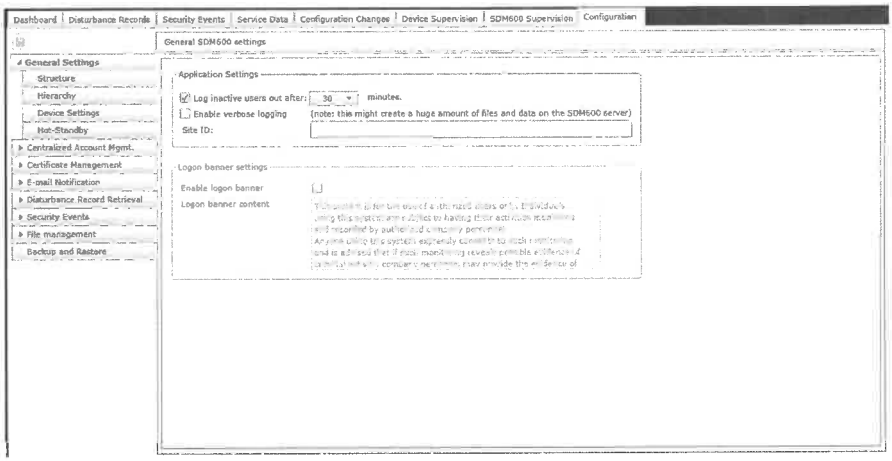


Figure 8.1: SDM600 Configuration Tab - General Settings

In General Settings, the following information can be configured:

- Enable automatic logout. It is possible to define that an SDM600 user is logged out after an inactivity of a pre-defined time period
- Enable verbose logging. When there is a problem, the verbose logging feature can be enabled to make SDM600 log nearly all operational events. By default, verbose logging disabled.

SDM600 provides operational logging functionalities. Operational error messages and additional information are logged during operation. The log file is stored under the installation folder of SDM600 , in other words, *<Operating system default drive>:\Program Files (x86)\ABB\SDM600*, if the default installation folder is selected. By default, it is located under *C:\Program Files (x86)\ABB\SDM600\log*.

- Enter SiteID information
- Enable and define logon banner. If this setting is active, text from logon banner content is displayed on the screen before SDM600 login window.

8.2 Setting Up SDM600

The configuration of SDM600 follows the basic steps as reflected in the subtab sequence in the Configuration Tab.

- The structure of the system under observation
- Hierarchical system configuration
- Device settings

8.2.1 Setting Up the SDM600 Structure

There are three ways to set up the system structure in SDM600:

- Manual configuration
- Import the system configuration file (IEC 61850 SCD file)
- Import system configuration for non IEC61850 devices (CSV file)

This function can be found in the **General Settings > Structure** subtab of the **Configuration** tab.

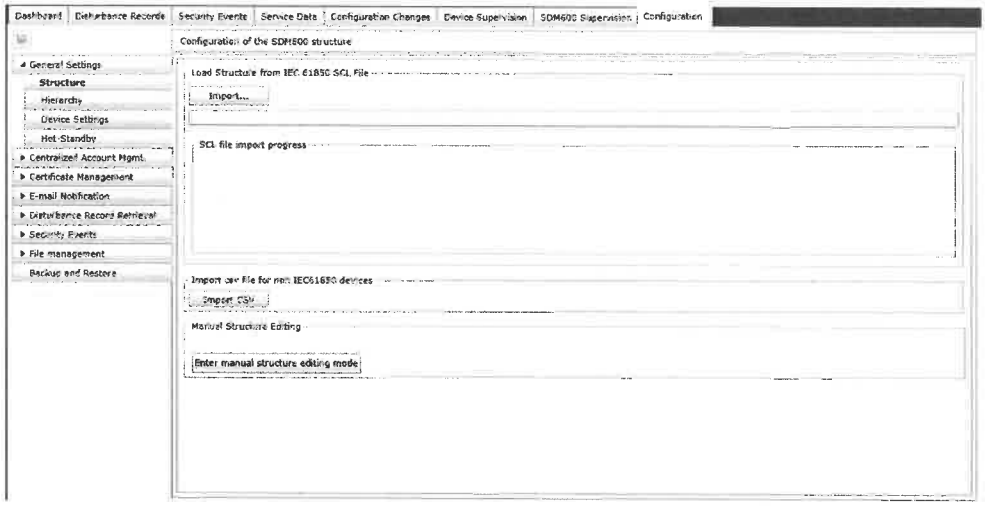


Figure 8.2: Configuration Tab in the SDM600

Remember to save changes after manual structure editing

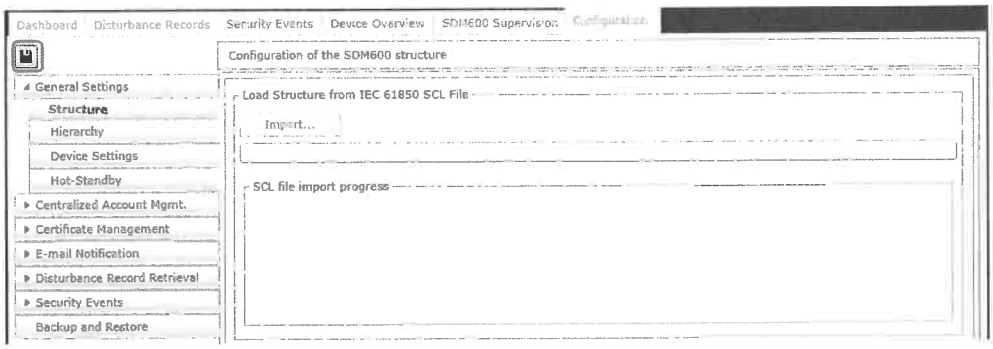


Figure 8.3: Save after manual structure editing

8.2.1.1 Manual Structure Configuration

To manually build the structure, do the following:

1. Open the **Go to the Manual Structure Editing** part in the **Configuration > Topology** subtab.
2. Click **Enter manual structure editing mode**.
   When entering the manual structure editing mode, the related parts of the UI are surrounded by a red border

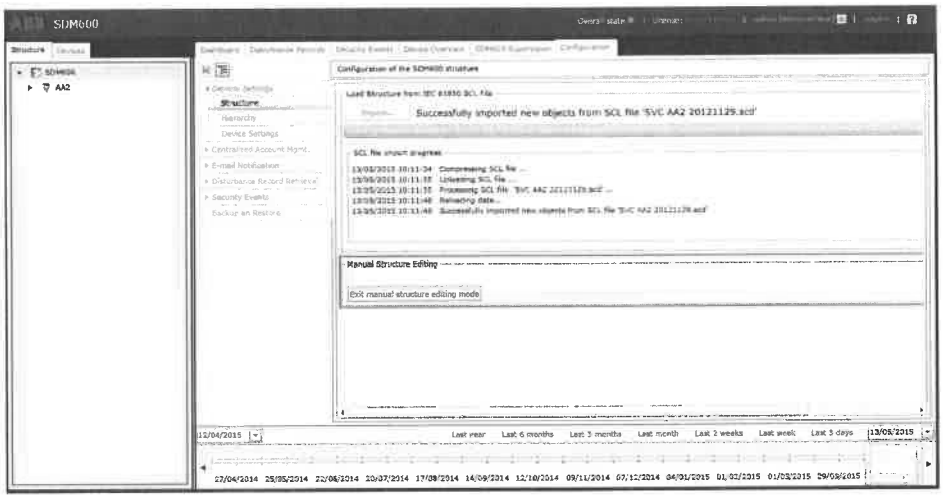


Figure 8.4: SDM600 Enter manual structure editing mode

3. Navigate to the Navigation Reference Area. Based on the selected entity, it is possible to create different types of sub-entities:
   - *Substation Group*: a virtual group of two or more substations. For example, it is possible to create a substation group for Region A that consists of Substation

A1, Substation A2, and so on. It is only possible to create substation entries directly under a substation group.

- *Substation*: a container for a substation. For example, to accommodate Substation A1, a substation entry called "Substation A1" can be created. It is possible to create Voltage Level and IED entries directly under a substation.
- *Voltage Level*: a container for different voltage levels under a substation. For example, under Substation A1, there can be two voltage levels: 110 kV and 220 kV. It is possible to create Bay and IED entries directly under the Voltage Level.
- *Bay*: It is possible to create IED entries directly under a bay.
- *IED/device*: a device in a substation. SDM600 prepares several commonly known IEDs in the default list. This list can be modified by adding or removing IED templates from the *IEDTemplates folder* of the SDM600 installation folder. To work on an IED template, see Step 4.
- *SDM600 Child*: an instance of SDM600 that this SDM600 is planning to connect to and retrieve necessary data from.

It is possible to rename each element that is added to the tree.

4. Add an IED or device. SDM600 comes with a pre-defined list of IED templates from multiple vendors. You can select from the list or, for an undefined IED, a custom type can be used.

   An IED template is an XML-based file that describes the IED type:

   - IED type name (for example, RE.670, RE.615, and so on)
   - Manufacturer of the IED (for example, ABB)
   - Supported protocols - IEC61850 MMS
   - Information whether the IED can have a disturbance record or not
   - Information on the directory location of the disturbance record

   By default, the IED templates are located in the IED Template folder in the SDM600 installation folder. For example, in the Microsoft Windows 7 x64 operating system, the IED template files can be found under *C:\Program Files (x86)\ABB\SDM600\IEDTemplates*.

   The SDM600 user can create a new IED Template for an IED that is not listed in the available list. The format of the XML schema is shown in the following figure. Only the part that is marked in yellow needs to be modified.

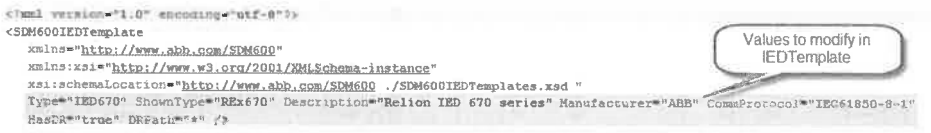


Figure 8.5: IED Template Format

To create a new IED template for a specific IED type, do the following:

a. Copy one of the IED Template files. The new file should be in the same location as the default IED Template files. Rename it accordingly. By default, it is named based on its type name/type family name.
b. Open the template file in an XML editor.

c. Fill in the mandatory Type attribute information. For example, *Type = "IED_NewType"*.

   It is highly recommended to fill in the Manufacturer attribute information, as well. For example, *Manufacturer="ABB"*. The strings defined for attributes *Type* and *Manufacturer* must match the strings defined in the *SCD* files that are originally delivered in the manufacturer's *ICD* or files. This is to ensure that when importing the IEC 61850 SCD file into SDM600, it matches the corresponding template files and the correct information of the IED can be shown and further used.

d. Fill in other attribute information such as ShownType, Description, ShownManufacturer, CommProtocol, HasDR, and the DRPath. Filling in this information means more information regarding the IED type is provided at the UI level.

   The HasDR attribute indicates that the IED in question can have a DR file. The DRPath attribute indicates the path to the DR files.

e. To see the newly created IED template, log out from SDM600 and log in again.

5. After the type of an IED or device is selected, a new node is added under the selected parent node.

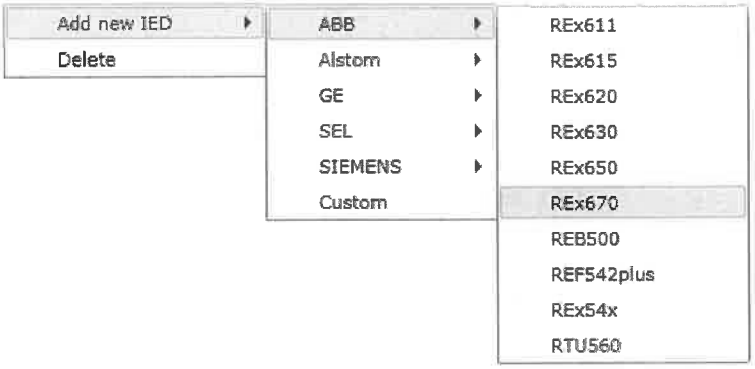


Figure 8.6: SDM600 Manual Configuration - Add new IED

6. If necessary, to change the name of an IED or device, double-click the name.

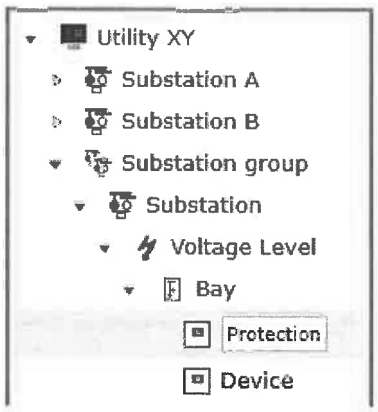


Figure 8.7: SDM600 Manual Configuration - Edit IED's Name

7. Repeat steps 4 – 6 to form a meaningful structure.
8. When the topology design activity is done, click **Save**.
9. Close the Manual structure editing mode.

8.2.1.2 Automatic Structure Creation

To automatically construct the SDM600 structure, from the SCL file, do the following:

1. In the **Configuration > Structure** tab, open the **Load Structure from IEC 61850 SCL file** part of the tab.
2. Click **Import**.
3. Load the SCL file by using the available dialog. First select an SCL file to be loaded, then click **Open** to load the SCL file to the SDM600 system.
   The state of the process can be seen in the import progress box.

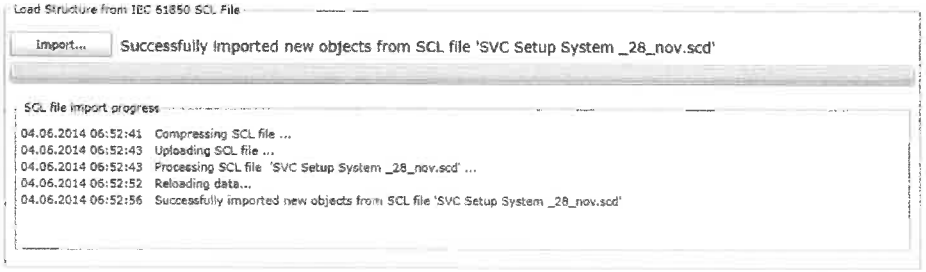


Figure 8.8: Configuration Tab - Topology Subtab - IEC61850 SCL file is loaded successfully

4. Next, the SCL file is uploaded and processed by SDM600.
   When the loading is finished, the new substation is added to the tree. The user is informed based on the status message at the top of the progress bar.

After the substation topology is imported from the IEC61850 SCL file, the tree view that represents the substation topology is automatically generated. To make the tree view easier to read, it is possible to edit the text that correlates to different parts of the tree. For example, instead of having "AA2" as a substation name, a user can edit the name and change it to "Substation Baden". To edit texts in the tree, do the following:

1. Click **Enter Manual structure editing mode**.
2. Navigate to the part of the tree where a text needs to be changed.
3. Double-click the node, and enter the new text.

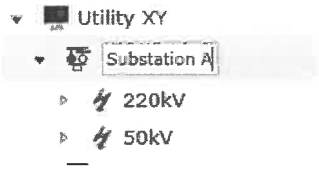


Figure 8.9: How to Edit Text on the Treeview

Every IEC61850 SCD file that is imported by SDM600 is treated as a new substation. This also applies to an IEC61850 SCD file that has been imported before.

Hoewer if IP address of imported device is already present in the SDM600 then this filed will be empty after import. It's possible to change IP address of each device in **Configuration > General Settings > Device Settings.**

Another way to add devices to SDM600 structure is to upload CSV file. Template for CSV file can be downloaded from **User and application settings > Downloads**

8.2.2 Setting Up SDM600 Hiearchical Function

SDM600 offers a hierarchical functionality as a way to integrate with other instances of SDM600 that are installed on another level of the organizational structure. For example, a standalone SDM600 that is installed at the network control center level can be integrated with one or multiple standalone SDM600 that are installed at the substation level. In this setup, the standalone SDM600 at the network control center level is further called as *SDM600 parent,* where the standalone SDM600 at the substation level is then called *SDM600 child.* With this integration, the SDM600 at the network control center level aggregates information from multiple substations and presents the information accordingly. The following figure shows a possible SDM600hierarchical deployment

scenario with an SDM600 parent at the network control center connected to the SDM600 children in the Substations A & B.

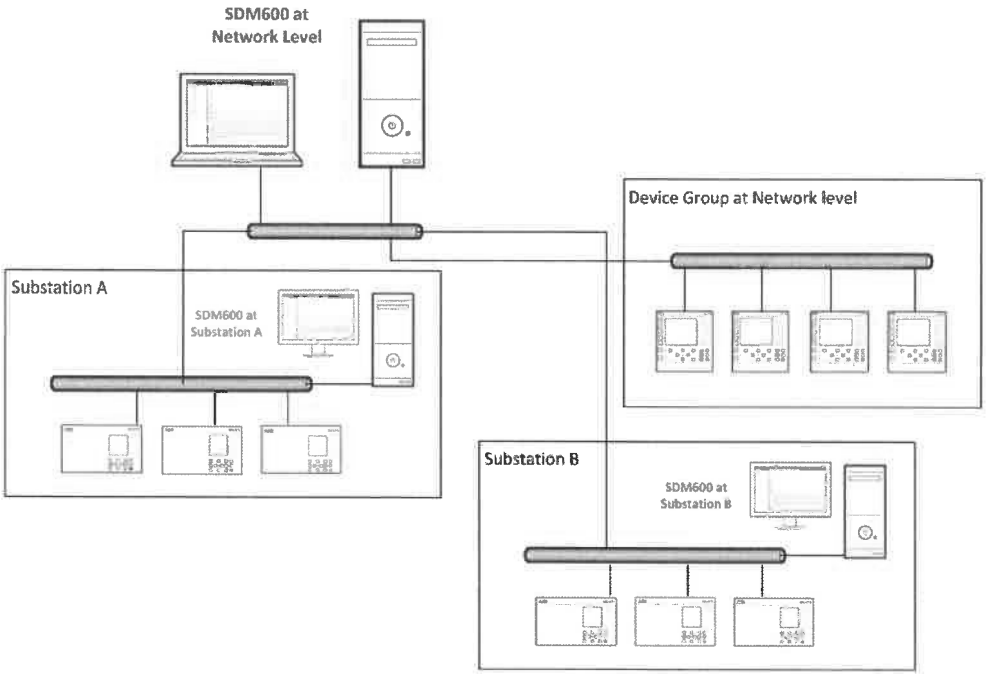


Figure 8.10: An Example of SDM600 Hierarchical Structure Deployment

To collect data from an SDM600 child device, the SDM600 parent requires the license for hierarchy mode. Without this license, it is not possible to add the SDM600 child.

It is important to back up the SDM600 child before establishing the hierarchical structure. In case of an unexpected result, it is easier to restore the configuration.

After creation of parent - child relation, it is very important to reactivate again the Central Account Management. Consequently, all devices that need authentication to SDM600 needs to be re-configured.

Before setting up the SDM600 hierarchy between an SDM600 parent and an SDM600 child, it is important that you ensure that the SDM600 servers have a dedicated IP addresses.

Make sure that "*Default Interface*" in **Configuration > Centrlized Account Mgmt.** is selected for the interface used for communication between parent and child.

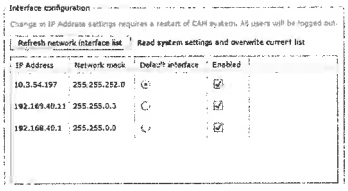


Figure 8.11: Interface configuration for hierarchical relation

It is important to ensure that the time between an SDM600 parent and an SDM600 child is synchronized. For instructions, see the Windows Operating System user manual.

To create a parent/child relationship between this SDM600 (parent) and a standalone SDM600 (will be the new child to this parent), do the following:

1. To add an SDM600 hierarchy, it is important to execute the following steps **on the SDM600 child** in the presented order:
   a. Navigate to **Configuration Tab > General Settings > Hierarchy** on the SDM600 child.
   b. Focus on the **Initial communication encryption** part.
   c. Enter a shared secret that is used to secure the communication between the SDM600 child and the SDM600 parent.

      To enable secure communication between the SDM600 parent and child for the first time, the shared secret has to be provided to both units. The shared secret is used to encrypt and decrypt the initial communication between the SDM600 parent and child. After the configuration is set up, the parent and child communicate by using transport layer security.

   d. Set the length the validity period of the temporary secure communication channel between the SDM600 child and parent. This secure channel is used to transport the SDM600 child configuration package from the SDM600 parent.

      It is not recommended to permanently open this temporary secure communication channel (by

selecting Always on Timeline Duration). In general, it is a cyber security principle to close any unnecessary communication channels. An exception can be accepted if the connection between the SDM600 child and parent is established by using a time-limited Virtual Private Network.

e. Click **Initialize Communication**.

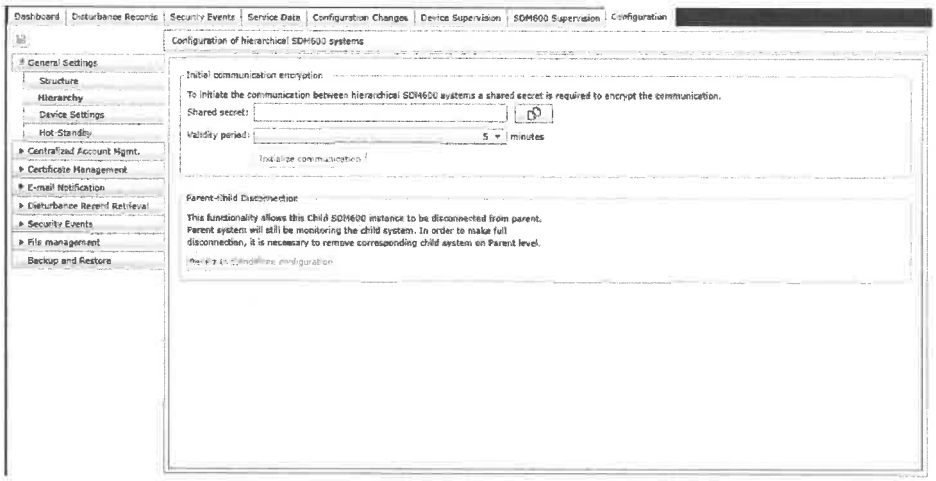


Figure 8.12: SDM600 Hierarchy Setup - Enter Initial Communication Encryption Details

2. As of this step on, all actions are conducted **on the SDM600 parent**. Start by navigating to **Configuration > General Settings > Structure** on SDM600 parent, and enable Manual Configuration by clicking on the button **Enter Manual structure editing mode**.
3. Navigate to the **Navigation Reference Area** and click the root SDM600 level.
4. Right-click with the mouse, and from the context menu, select **Add New SDM600 Device**.

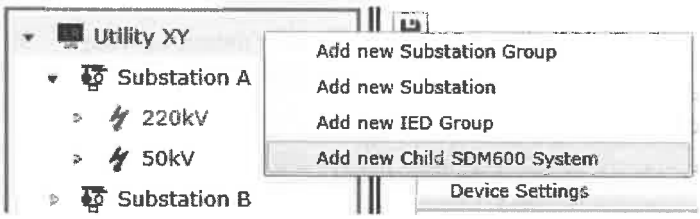


Figure 8.13: SDM600 Context Menu - Add SDM600 Child Device

5. In the dialog box, fill in the relevant information, then click **Add**. Click **Save** to commit the changes.

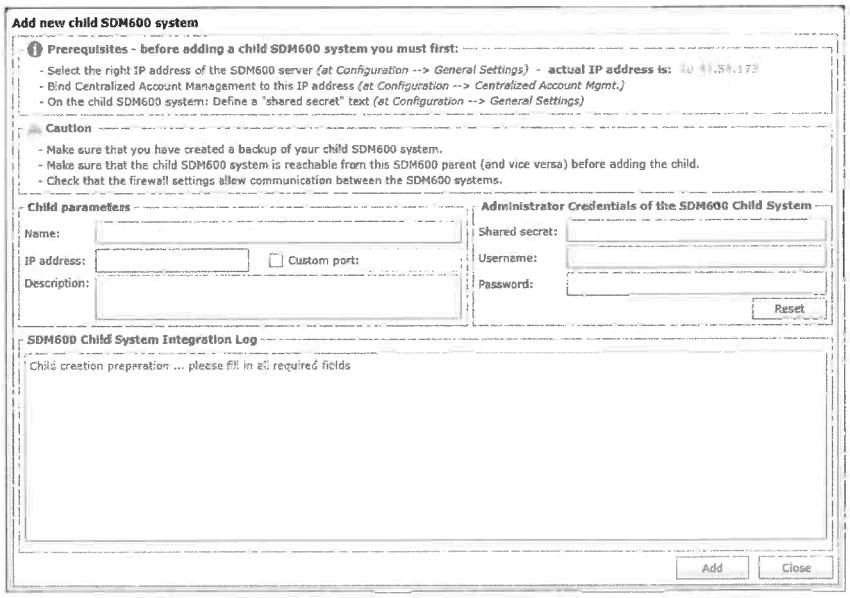


Figure 8.14: Add SDM600 Child Device Dialog Box

To integrate a child SDM600 successfully, the following information needs to be provided:

- The IP address of the child SDM600
- The port number if the child SDM600 is not using a default port number
- The user credentials of the child SDM600 that has administrator rights. If there is no access to the child SDM600, your user administrator needs to create a temporary administrator user for this integration.
- The shared secret. The shared secret has to be the same as the one that is entered on the child SDM600.

6. When an SDM600 child is successfully added to the structure, it is shown in the tree structure and also in the **Configuration Tab > Hierarchy** subtab.

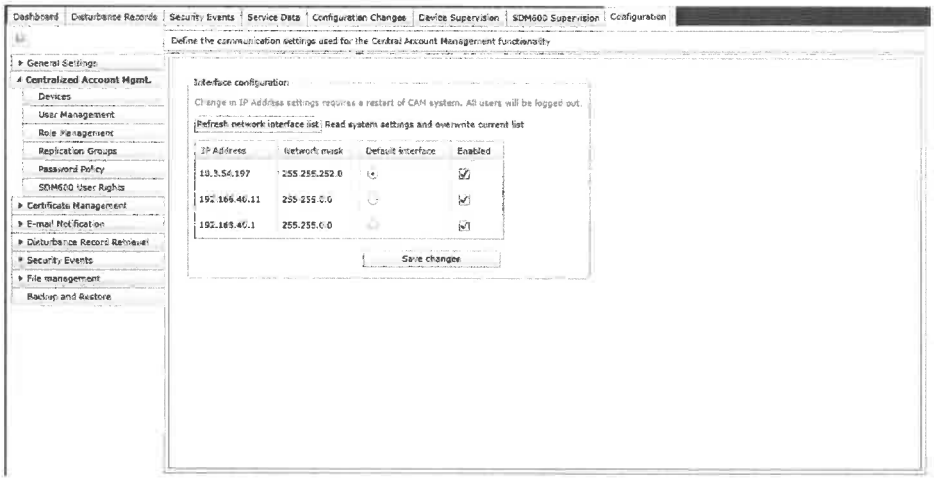


Figure 8.15: SDM600 Child Device successfully added to the system

If connected child is working in Hot Standby relation, then IP address of the child's partner system (hot or standby) is presented in *Partner System IP address* column.

7. Log out from parent, after establishing parent child relation.
8. To add another SDM600 child, repeat steps 1-7.
   If the integration of an SDM600 child into the SDM600 hierarchy fails, revert the SDM600 child to a standalone SDM600 before another integration attempt.

After establishing a hierarchy relationship between the SDM600 parent and child, the following behaviour is expected on the SDM600 child:

- As the account management functionality at the SDM600 child is now integrated to the SDM600 parent, it is no longer possible to manage users on the SDM600 child. Also, any user changes that are made at the SDM600 parent are reflected directly on the SDM600 child.

When the hierarchy structure is established between the SDM600 parent and child, the centralized account management of the SDM600 child is integrated to the SDM600 parent. This implies that any user accounts previously created on the SDM600 child are no longer available. The user accounts on the SDM600 child will be the same as on the SDM600 parent. Any account changes made on the SDM600 parent will

automatically be reflected on any SDM600 children. In addition to that all centralized account management certificates created on child have to be regenerated and uploaded to devices.

When setting up the SDM600 hierarchy, it is important that the network connection between the SDM600 parent and child is not disturbed. If there is disturbance, transporting the SDM600 child package may fail or the SDM600 parent may not receive feedback from the SDM600 child. In this case, it can be seen on the SDM600 parent that the establishment of the hierarchy fails.

In addition, as the configuration file changes the behaviour of the SDM600 child, all related SDM600 services on the SDM600 child are restarted. In general, restarting of the services should work fine. If it fails, the SDM600 parent receives a notification that the establishment of the hierarchy has failed.

If the establishment of the hierarchy has started and fails, it is also possible that the SDM600 child can no longer be accessed using the original user accounts. This is because the user management part of the SDM600 child has been successfully integrated to SDM600 parent's centralized account management. Therefore, you can try to log in with a user from the SDM600 parent.

When the establishment of the hierarchy fails, it is not possible to directly add the same SDM600 as a child. At this stage, it is important to revert the SDM600 child to a standalone SDM600, log out from parent anch child and log in again before trying to establish the hierarchy again.

Notice that replication between parent and child may take time. It's strongly recomended to wait about 5 minutes before log in to SDM600 after hierarchy relation is established.

If a user would like to cancel the hierarchical (parent - child) relationship between one SDM600 and another SDM600 completely, the user should first **remove the SDM600 Child entry in the SDM600 Parent unit**. This can be done by following the steps below:

1. Navigate to **Configuration > General Settings > Structure** , and enable Manual Configuration by clicking on the button **Enter Manual structure editing mode**.
2. Navigate to the **Navigation Reference Area** and click the SDM600 Child unit that is to be deleted.
3. Right-click with the mouse, and from the context menu, select **Delete**.
4. When it is done, remember to navigate out from the manual structure editing mode.
5. Click **Save** to commit the changes.

Secondly, SDM600 provides a reverse function to set the SDM600 Child status to become a standalone SDM600. This function can be used only when disconnecting on parent is done (see abowe) or parent system has been dismissed.

After the reversion, the SDM600 parent will no longer be able to connect to the SDM600 child. Furthermore, the user account management on the SDM600 child is no longer synchronized with the SDM600 parent.

To revert the state of an SDM600, navigate to **Configuration > Centralized Account Management**. Click **Revert to standalone configuration** button. Enter the SDM600 administrator username and password. After this, restart the PC.

In order to have a clean termination between SDM600 Child unit and SDM600 Parent unit (when the disconnection was initiated on SDM600 Child), the aforementioned steps on SDM600 Child unit and SDM600 Parent unit have to be executed completely.

The reverse function is a critical function and should be executed with extra care. Therefore, only an SDM600 administrator can perform such a function by means of extra authentication. This implies that, even if users are granted access to the SDM600 configuration, they do not necessarily have the right to execute this function. When clicking the button, an additional user verification dialog is shown. The user has to enter the SDM600 administrator credentials. Only if the authentication is successful, the revert function is executed.

8.2.3 Setting Up the IEDs/Devices

In general, all the IED or device settings are available in the loaded SCD files. However, when some IED or device information needs to be edited, users can navigate to the **Configuration tab > General Settings >Device settings** subtab. In this subtab, it is possible to edit the following information:

- *Name*: the name of the IED or device
- *Description/Customized name*: a description of the IED or device
- *Comment*: a placeholder for comments on a device
- *Type*: the type of the IED or device
- *IP Address*: the IP address that the IED or device is bound to
- *NERC-CIP Rating*: shows importance of the device in the substation.
- *Property protocol*: allows to configure protocol used for reading device's configuration changes and service data.
  Possible values are:
  - IEC 61850-8 - allows to read service data from devices using IEC 61850-8 protocol
  - SNMPv1 - allows to read service data from devices using SNMPv1 protocol
  - SNMPv2 - allows to read service data from devices using SNMPv2 protocol
  - SNMPv3 - allows to read service data from devices using SNMPv3 protocol
  - HTTP Client - allows SDM600 read client information based on http request header
  - Windows Client - allows to read MS Windows information using Windows Agent

    Windows Agent is a standalone tool for MS Windows systems. It's collecting and dending to SDM600 OS specific information like version, hardware information, antivirus and installed OS patches. Windows Agent Installer can be donloaded from the **Downloads** tab in **User and Application Settings**

  - RTU Web API - allows to read ABB RTU rel. 12 or newer
  - None
- *Service Data Protocol Configuration* - allows to set up protocol specific properites like login name, password or authentication method. This option appears only if choosen protocol requires additional properties and after saving changes.
- *Custom properties* - this option is available only for SNMP v1, v2 and v3 protocols. After clicking on *Configure* link the new window is opened.
  There are two tabs on newly opened window:
  - *Custom Properties for Device* - allows to map SNMP device properties with SDM600 device properties.
  - *System Properties for Protocol* - a list of predefined system properties.

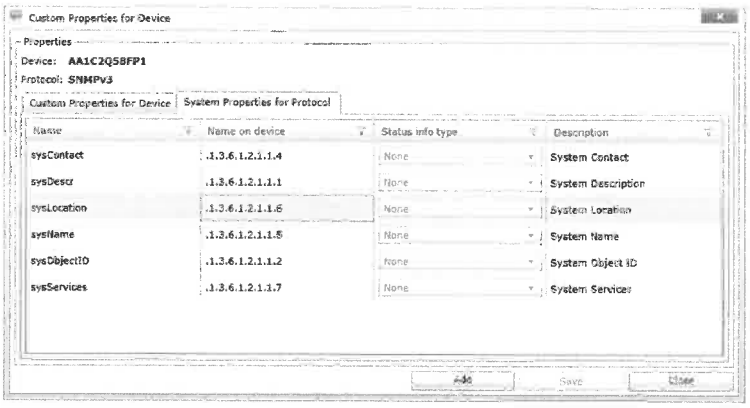


Figure 8.16: SNMP Custom Properties for Device

- *Configuration Tool*: allows to set up configuration tool for the device. This value can be set to local path or http/https address. As default SDM600 is using https connection to the device IP address. After clicking on *Configure tool*, new window is opened.

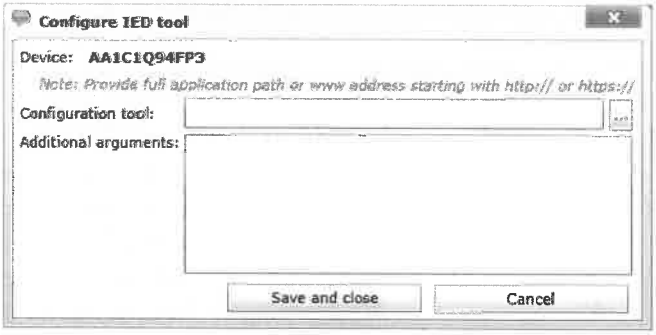


Figure 8.17: Configuration tool window

In *Configuration tool* field is possible to enter http or https address or provide path to tool installed on the drive.

In order to be able to run configuration tool form local path, tool have to be installed on the server and on all SDM600 clients in the same path on corresponding drives.

If configuration tool link will open Web based configuration tool, full URL have to be provided (strating with *http://* or *https://*

- *Properties*: allows to manually overwrite service data information gathered form the device.
- *Contains DR Function*: to indicate whether the IED or device has the disturbance record functionality.
- *Manually Created*: idicates that device has been configured form structure import or manually
- *Poll cycle(sec)*: Defines minimum time when SDM600 can connect to the device in order to poll data.

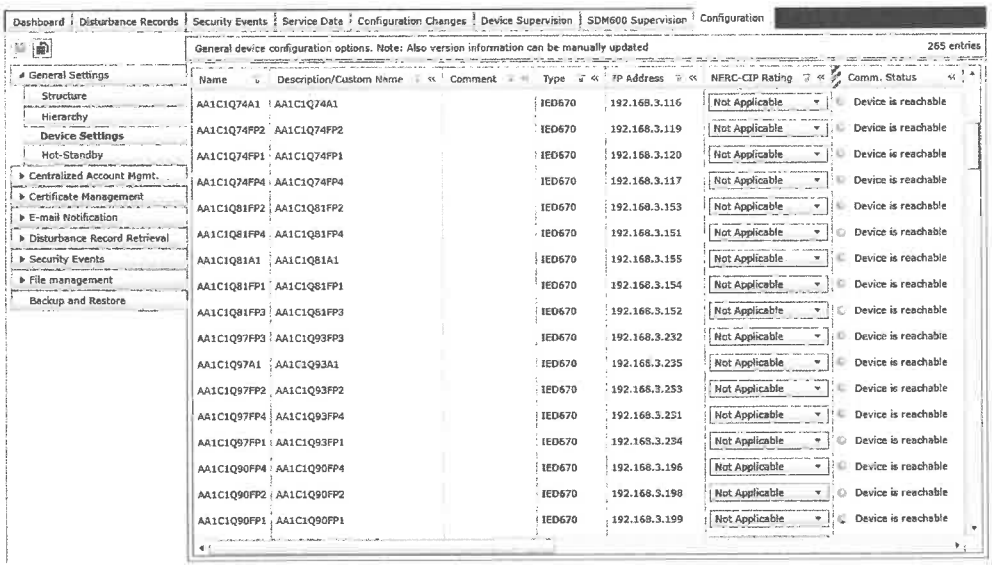


Figure 8.18: SDM600 Configuration - IED Settings

To edit the information, double-click the cell where the information to be changed is. The changes take effect once they are saved.

The information mentioned in this section should be edited with care. Misconfiguration on the IED information properties may cause SDM600 to lose connectivity to the IEDs.

IED / device information that is edited in this subtab is stored only in SDM600. Furthermore, IEC 61850 related information will be overwritten with the latest value from the device when SDM600 is connected to the device.

8.2.4 Setting Up SDM600 Hot Standby Function

SDM600 offers a hot standby functionality to increase the availability of the overall SDM600.

A hot standby is a failover mechanism to provide maximum reliability with outstanding convenience at the same time in SDM600 system. The hot unit is the active unit and in the normal operation is considered as a working system. If any of the key component in the hot unit fails, the standby unit will immediately take over the operation.

In SDM600, the hot standby function enhances overall system functionality by providing the following attributes:

- Fully automated synchronization of all relevant data between hot and standby unit
- Integrated self-tests for checking system status
- Automatic failover if internal errors is detected
- Easy setup and configuration of the hot standby redundancy functionality

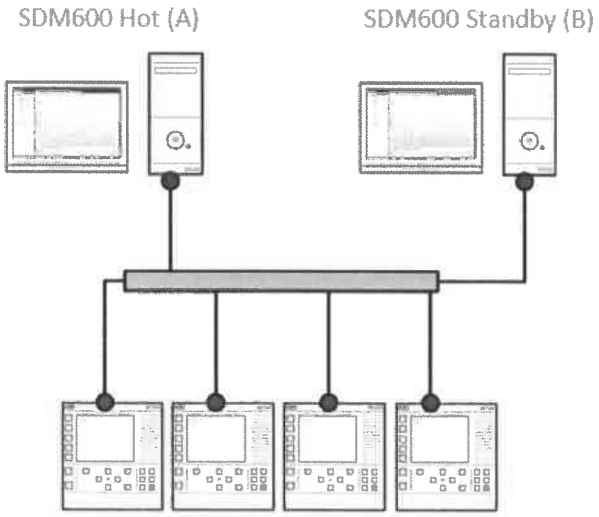


Figure 8.19: SDM600 hot standby structure

After configuring of hot standby functionality, all data from hot unit will be mirrored to standby unit. It means that all existing data on standby unit will be replaced by data from hot unit.

It is important to back up the SDM600 before establishing the hot standby relation. In case of an unexpected result, it is easier to restore the configuration.

To setup the hot standby function between two SDM600, do the following:

1. Configure an SDM600 (B) to become a standby unit. It is important to execute the following steps on the SDM600 standby unit in the presented order:
   a. Navigate to **Configuration Tab > General Settings > Hot Standby**
   b. Click on **Create Hot-Standby System**
   c. Enter a shared secret that is used to secure the communication between the SDM600 hot unit and the SDM600 standby unit

      To enable secure communication between the SDM600 hot unit and standby unit for the first time, the shared secret has to be provided to both units. The shared secret is used to encrypt and decrypt the initial communication between the SDM600 hot and standby units. After the configuration is set up, the hot and standby units communicate by using transport layer security.

   d. Set the validity period of the temporary secure communication channel between the SDM600 hot unit (A) and standby unit (B). This secure channel is used to transport the SDM600 standby unit configuration package from the SDM600 hot unit.

      It is not recommended to permanently open this temporary secure communication channel (by selecting Always on Timeline Duration). In general, it is a cyber security principle to close any unnecessary communication channels. An exception can be accepted if the connection between the SDM600 standby unit and hot unit is established by using a time-limited Virtual Private Network.

   e. Click **Initialize**.

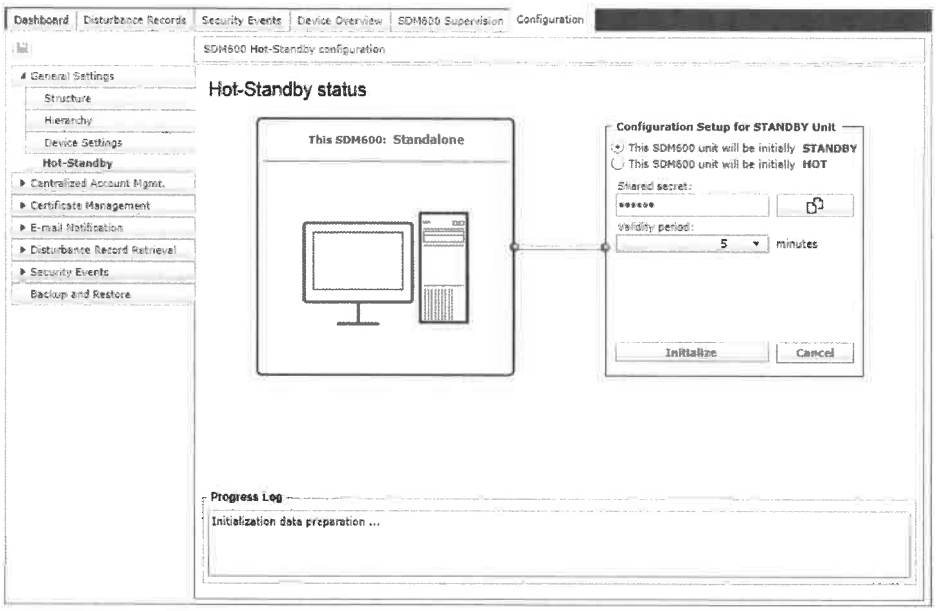


Figure 8.20: Set SDM600 as a standby unit.

2. On the SDM600 unit that is designated to become a hot unit (A), follow the next steps in the presented order:

   a. Navigate to **Configuration Tab > General Settings > Hot Standby**
   b. Click on **Create Hot-Standby System**. A small dialog window will be opened
   c. Select **This SDM600 unit will be initially HOT**
   d. Enter the shared secret that is also entered at the SDM600 standby unit
   e. Enter the IP address of the SDM600 standby unit
   f. Enter the port number of the SDM600 standby unit
   g. Click on **Initialize** to start the hot standby pairing process

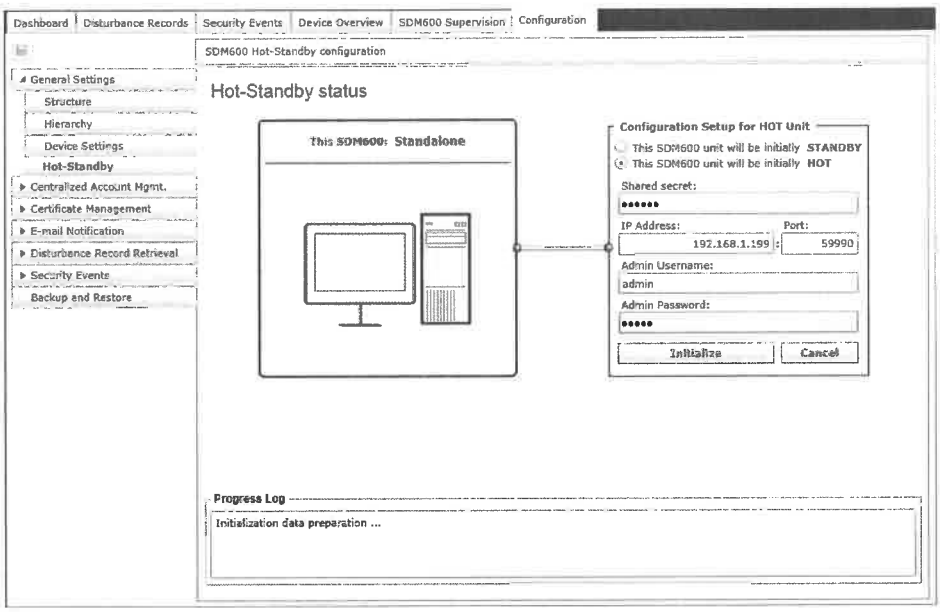


Figure 8.21: Set SDM600 as a hot unit.

Depending of the size of the database files, replication may take some time. Unless replication is done, Hot Standby is not fully operatible. Be patient.

To activate the Hot Standby feature, the assigned SDM600 peer has to be in the same network as the installed SDM600 and time on both machines has to be synchronized.

In SDM600 Hot Standby function, there is no fix definition in defining that a unit is hot or standby. Initially, the user has to define which unit is set to hot and standby.

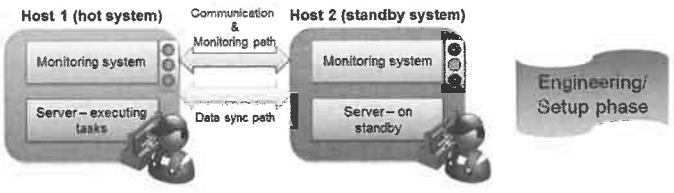


Figure 8.22: Hot and Standby Definition in SDM600 Hot Standby Redundancy functionality

After the definition is set, if both units are shut down, then unit, where first user will log in to SDM600 becomes the hot unit.

8.2.5 Revert to Standalone Systems from Hot Standby

In order to disconnect SDM600 systems from Hot-Standby relation follow below steps

1. Navigate to **Configuration Tab > General Settings > Hot Standby**
2. Click on **Revert to Standalone SDM600** button.

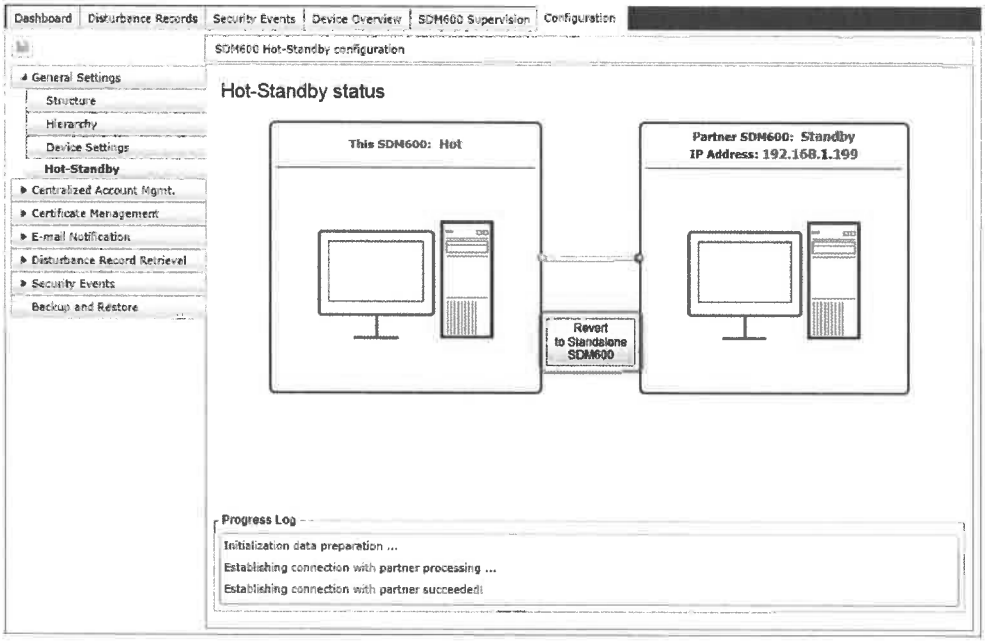


Figure 8.23: Hot Standby disconnection

After disconnection, restart partner machine (former standby).

Cancelling the Hot Standby function has to be done with extra caution. Disabling this feature means the SDM600 returns to a stand-alone mode and thus, there is no backup when the installed SDM600 is encountering problems. It's recommended to create a backup after successful hot-standby disconnection.

Notice that all information are deleted from disconnected standby unit.

8.2.6 Centralized Account Management

The SDM600 provides central user account management functionality with Role Based Access Control (RBAC) Management for devices supporting:

- IEC 62351-8 (Pull Model, Profile A)
- RADIUS (RFC 2865) devices
- Windows PC
- MicroSCADA

This feature enables SDM600 to centrally manage users on different devices, applications and systems. This feature benefits both the users and the administrator of the system that is managed by SDM600. For the administrator, the feature enables access control on every device without being exposed to the complexity of credential management on every device or application in the system. The users have to remember only one credential when accessing devices or applications that authenticate the users against the SDM600 server. In addition, for both the administrator and users, changing of credentials can be done directly from SDM600 and the change becomes effective immediately on the connected devices and systems. Furthermore, the SDM600 centralized account management is more than just credential management. A user can be assigned one role or multiple roles. From SDM600, the administrator or an authorized user can assign IEC 62351 pre-defined or custom defined roles to users. RBAC allows a user to select the role that is appropriate for the current task/job, thus preventing the possibility of the user unwittingly making changes or performing unwanted operations. This also ensures that users can only perform the tasks they are authorized to perform. The design of the centralized account management in SDM600 is based on IEC 62351-8 on Role-based access control.

The Centralized Account Management functionality is configured as follows:

1. Activate Centralized Account Management in SDM600.
2. Assign a Role or Roles to each user.
3. Define the user role to rights mapping for SDM600 application.

8.2.6.1 Centralized Account Management Setting

The Centralized Account Management setting provides the following functions to the user:

- Enable nertwork interface for SDM600 Centralized Account Management. This setting instructs SDM600 to set the centralized account management functionality on a defined IP addresses. SDM600 is automatically trying to distiguish corect network interface for every device. If this is not possible then interface maked as

default is taken. In addition to that *Default interface* shall be selected for the interface used for parent-child or hot-standby connection.

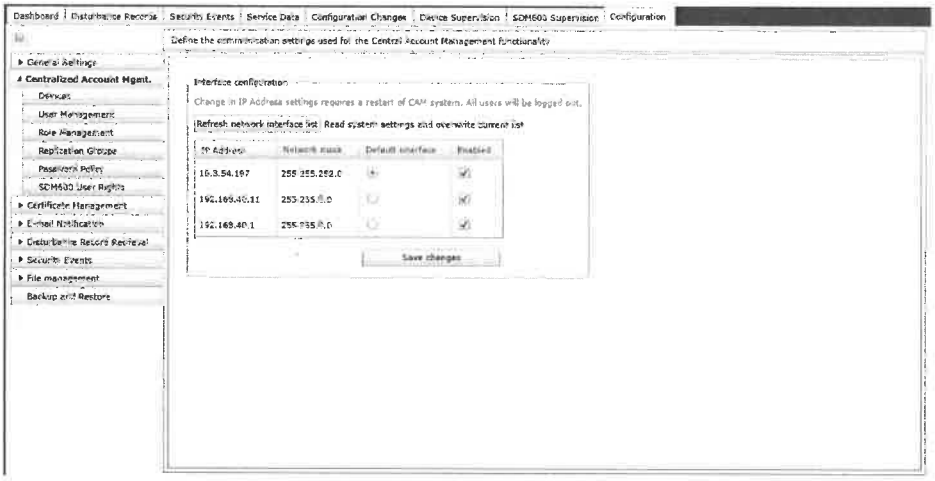


Figure 8.24: SDM600 Configuration - Bind to Other IP Address

- Generate user authentication configuration file for devices. This function allows users to download the user authentication configuration file for a device or application that wants to get benefit from using SDM600 centralized account management.
- Manage users accounts. This function allows to add and delete users accounts. Administrator can reset password for selected user.
- Manage replication groups. This function allows to replicate to the device only selected groups of users. This is decreasing replication time and also saving device memory.
- Define password policy. This function allows to increase accounts security by enforcing password policies and rules.
- Set users rights. This function allows to define rights for selected roles.

8.2.6.2 Create CAM configuration package for device

In order to create CAM package for application or device to use SDM600 centralized account management, the user needs to:

1. Make sure that SDM600 is binded to correct IP address
2. Navigate to **Configuration > Centralized Account Mgmt. > Devices** subtab.
   - Download the configuration to replicate complete SDM600 users

   This is only possible for particular applications or devices from ABB.

3. Select device or devices for which CAM configuration will be generated.

4. Click on **Add new CAM Configuration** button.

Figure 8.25: Add new CAM Configuration button

5. Select IEC62351 Protocol.

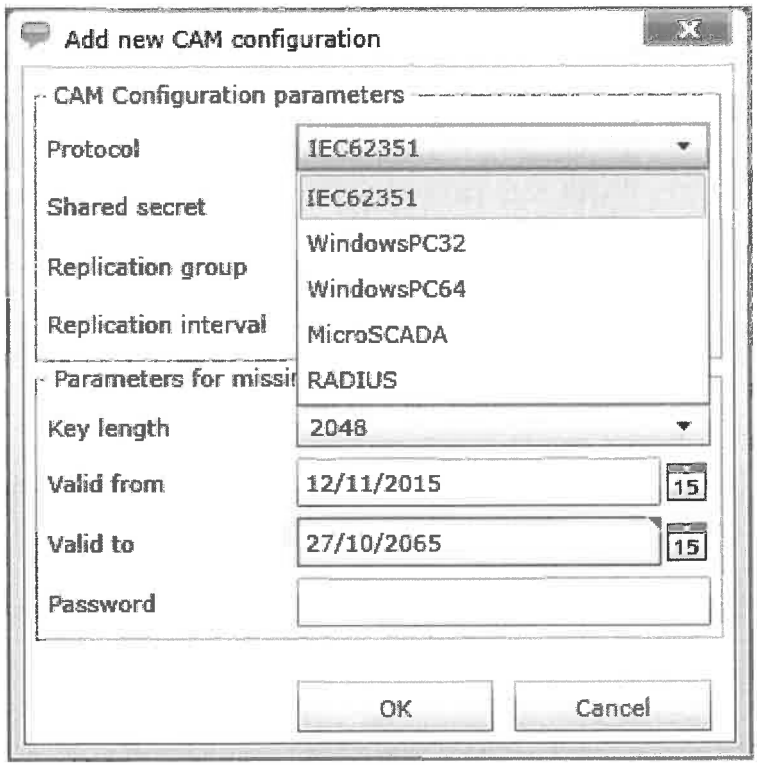


Figure 8.26: Add new CAM configuration protocols

6. Define certificate key length, validity dates and certificate password.

If CAM package is generated for multiple devices in one step, then password for generated certificates will be the same.

Longer certificate key is increasing security, but too long key may impact device performance. Recommended value is 2048 bits.

7. Save newly created CAM package by hitting **Save** icon.
8. Copy CAM packge for selected device or devices.

Figure 8.27: Copy CAM package button

8.2.6.3 Integrating RADIUS devices into SDM600 Centralized Account Management

As a centralized account management unit, SDM600 provides the functionality to integrate RADIUS devices into its account management functionality. This means that devices that use RADIUS authentication can be centrally authenticated to the SDM600 centralized account management.

Configuration of RADIUS device is very similar to configuration of IEC62351 device. To enable this, it is important to register the RADIUS device as a device in SDM600

To register the devices, do the following:

1. Navigate to **Configuration > Centralized Account Mgmt. > Devices** subtab.
2. Select device or devices which will use RADIUS for authorisation.
3. Click on **Add new CAM Configuration** button.

Figure 8.28: Add new CAM Configuration button

4. Select RADIUS protocol.
5. Provide shared secret

It is important to specify the shared secret that is a text string that serves as a password between a RADIUS device and the SDM600 centralized account management.

RADIUS shared secret is used to protect user passwords and the authentication of the SDM600 centralized account management replies. Therefore, if a user provides a shared secret that is not equal, the overall authentication process from the RADIUS device to the SDM600 centralized account management will not work properly, and vice versa.

SDM600 provides the possibility to retain the shared secret when entering the RADIUS client to SDM600.

6. Click **OK**
7. Click **Save** icon

On a RADIUS device, it is also important to set up the authentication mechanism to point to SDM600. Each RADIUS device has a different way of setting up such authentication mechanism. Please refer to the user manual or installation guideline of the RADIUS device.

Some RADIUS devices may require a Vendor Specific Attribute. However, in the current version of SDM600, SDM600 supports RADIUS devices that assign type of service the user has requested to the Attributes Service-Type. Normally, definition of each Attributes Service-Type can be found in the user manual of the RADIUS device.

SDM600 has a predefined mapping of Roles to the RADIUS Attributes Service-Type. This means that the RADIUS device can determine the user's Authorisation (rights) according to the user's role. This means if the RADIUS device supports the Attributes Service-Type for authorisation, then the tasks/operations that the user can perform in that device are defined by the role or roles assigned to the user. Each RADIUS device vendor may have a different definition of what does a specific Attribute Service-Type mean in its device. For example, ABB AFS Switch defines Attribute Service-Type [1], Service-Type [6] and Service-Type [7] as Operator, Administrator and Guest respectively.

The default mapping between SDM600 Roles and the RADIUS Attributes Service-Types is shown in the next Table.

Table 8.1: Default Mapping of SDM600 Roles to the RADIUS Attributes Service-Type

SDM600 Roles	RADIUS Attribute Service-Type
Viewer	Service-Type [7]
Operator	Service-Type [1]
Engineer	Service-Type [6]
Installer	Service-Type [6]
SECADM	Service-Type [6]
SECAUD	Service-Type [6]

SDM600 Roles	RADIUS Attribute Service-Type
RBACMNT	Service-Type [7]
Administrator	Service-Type [6]

In SDM600, a user may be assigned to multiple roles. In this case, when the user accesses a RADIUS device, the user will be assigned a corresponded RADIUS Attribute Service-Type that belongs to the most priority role. For instance, if the user has Administrator and Operator roles, the user gets the RADIUS Attribute Service-Type that correlates with the role Administrator since this is the most priority role, which in the default mapping is Service-Type[6].

The users have the possibility to customize the mapping to the users' needs. In order to adapt the mapping, execute the following steps:

1. Open the file CAMRoleToRadiusRights.xml where the original SDM600 mapping is stored. By default, it is located under the installation directory (in 64-bit Operating System, it is under C:\Program Files (x86)\ABB\SDM600\bin).
2. There are two major sections that are related to the mapping. These two major sections are *RoleDefinitionRadiusRight specific for IEC 62351* section and *RoleDefinitionRadiusRight specific for ABB* section. The users can navigate to the section where the role mapping adaption is to be done.
   - *RoleDefinitionRadiusRight specific for IEC 62351* section defines the mapping from the standard IEC 62351 roles to RADIUS Attributes Service-Type.
   - *RoleDefinitionRadiusRight specific for ABB* section defines the mapping from the ABB specific role (i.e. Administrator role) to RADIUS Attributes Service-Type.
3. Inside each *RoleDefinitionRadiusRight* section, there is one *RoleToRight* section and inside the *RoleToRight* section, there are multiple *RoleToRadiusRight* sections. Each *RoleToRadiusRight* section represent a mapping between a known SDM600 role to a particular RADIUS Attributes Service-Type. The *RoleToRadiusRight* section is composed out of two sections, namely *Role* section and *Rights* section. In order to modify the role to right mapping, the users can add or delete the respective RADIUS Attributes Service-Type (or also the Vendor Specific Attribute).

See the following examples. Assuming that a user would like to assign a RADIUS Attributes Service-Type *Service-Type[6]* from IEC 62351 role Engineer to IEC 62351 role Operator, the user can edit the respective part in the CAMRoleToRadiusRights.xml file. The next table shows the before and after adaptation of the mapping. Note that the table only shows a particular snapshot of the file's content.

It is required to restart the computer where SDM600 is installed after the re-mapping action between SDM600 Roles and RADIUS Attributes Service-Type is done.

Table 8.2: How to Customize the Mapping Between SDM600 Roles and RADIUS Attributes Service-Type

Default mapping from SDM600	Customized mapping by user
<RoleDefinitionRadiusRight> <RoleDefinition> <Revision xsi:nil="true" /> <Definition>IEC62351-8</Definition> <Roles /> </RoleDefinition> <RoleToRight> <RoleToRadiusRight> <Role> <Name>Viewer</Name> <RoleId>0</RoleId> </Role> <Rights> <string>Service-Type[7]</string> <string>RuggedCom-Privilege-level[guest]</string> </Rights> </RoleToRadiusRight> <RoleToRadiusRight> <Role> <Name>Operator</Name> <RoleId>1</RoleId> </Role> <Rights> <string>Service-Type[1]</string> <string>RuggedCom-Privilege-level[operator]</string> </Rights> </RoleToRadiusRight> <RoleToRadiusRight> <Role> <Name>Engineer</Name> <RoleId>2</RoleId> </Role> <Rights> ***<string>Service-Type[6]</string>*** <string>RuggedCom-Privilege-level[admin]</string> </Rights> </RoleToRadiusRight> . . . </RoleDefinitionRadiusRight>	<RoleDefinitionRadiusRight> <RoleDefinition> <Revision xsi:nil="true" /> <Definition>IEC62351-8</Definition> <Roles /> </RoleDefinition> <RoleToRight> <RoleToRadiusRight> <Role> <Name>Viewer</Name> <RoleId>0</RoleId> </Role> <Rights> <string>Service-Type[7]</string> <string>RuggedCom-Privilege-level[guest]</string> </Rights> </RoleToRadiusRight> <RoleToRadiusRight> <Role> <Name>Operator</Name> <RoleId>1</RoleId> </Role> <Rights> <string>Service-Type[1]</string> ***<string>Service-Type[6]</string>*** <string>RuggedCom-Privilege-level[operator]</string> </Rights> </RoleToRadiusRight> <RoleToRadiusRight> <Role> <Name>Engineer</Name> <RoleId>2</RoleId> </Role> <Rights> <string>RuggedCom-Privilege-level[admin]</string> </Rights> </RoleToRadiusRight> . . . </RoleDefinitionRadiusRight>

8.2.6.4 Integrating Windows PC Authentication into SDM600 Centralized Account Management

As a centralized account management unit, SDM600 provides the functionality to integrate Windows PC authentication into its account management functionality. This functionality is to allow users of Windows PCs that are in a workgroup to be authenticated against and managed by the SDM600 Centralized Account Management system.

If the Windows PC is part of a domain, the Windows users will be managed by and authenticated against Microsoft Active Directory (and not by SDM600)

To enable this, the user has to download the installer to be installed on the Windows PC. This installer is generated when Windows PC option is choosen during creation of Centralized Account Management package.

1. To benefit from this feature, the Windows PC has to be registered as a device in SDM600.
2. Navigate to **Configuration > Centralized Account Mgmt. > Devices** subtab.
3. Select device or devices which will use Windows PC Authentication.
4. Click on **Add new CAM Configuration** button.

Figure 8.29: Add new CAM Configuration button

5. Select WindowsPC32 or WindowsPC64 protocol. The available options are 32-bit or 64-bit operating system.

In order to find out the version of the installed Operating System on the Windows PC, open the Windows Explorer. Right click Computers and then select Properties. Information about the version of the installed Operating System can be found under System section – System Type.

6. Provide certificate validity dates and password.
7. Click **OK**
8. Click **Save** icon
9. Download installer on local computer by clicking **Download configuration package** icon.
10. Bring the file to the Windows PC on which the installer is to be installed.
11. Unzip the download package into a directory.

12. Run the installer.

The installer is tailored to this particular Windows PC. Installing the installer that is generated for another device will cause the integration of the Windows PC to the ABB SDM600 centralized account management to not work properly.

13. When the installation is completed, restart the Windows PC.
14. When the Windows PC is up and running, a new login page is shown.
    Now the user can log in into the Windows PC using the same credentials as in SDM600.

For new users that have just been created in SDM600, it is important that they change their password before logging into the PC via ABB SDM600 Centralized Account Management for Windows PC. A local profile in the Windows PC will only be created when the user enters a valid and updated password.

ABB SDM600 Centralized Account Management for Windows PC provides a way to change the mapping between a SDM600 Centralized Account Management role and a Windows operating system group. To change this mapping, navigate to your installation directory of ABB SDM600 Centralized Account Management for Windows PC and open the *GroupRoleMappingStore* file using administrator rights. The file can be opened by using a simple text editor or an XML editor.

An example of mapping can be seen as follows. In this example, the SDM600 Viewer and Operator Roles are mapped to "Some Windows Users Group".

```
<GroupRoleMapping>
<GroupName>Some Windows Users Group</GroupName>
<RoleDefinitions>
<RoleDefinition>
<Revision xsi:nil="true" />
<Definition>IEC62351-8</Definition>
<Roles>
<Role>
<Name>Viewer</Name>
<RoleId>0</RoleId>
</Role>
<Role>
<Name>Operator</Name>
<RoleId>1</RoleId>
</Role>
</Roles>
</RoleDefinition>
</RoleDefinitions>
```

```
</GroupRoleMapping>
```

Do the following:

1. Define an intended specific group role mapping. This can be done by specifying the tags <GroupRoleMapping></GroupRoleMapping>.
2. Within the <GroupRoleMapping> tags, you need to add the following information as seen in the previous example:
   - Define a new tag <GroupName></GroupName> that specifies the name of the Windows User Group. The "Group Name" node consists of the name of the Windows Users Group. Windows User Groups can be found in the system by navigating to the "Local Users and Groups" application. Go to **Windows Control Panel > Edit Local Users and Groups**.
   - Define a new tag <Revision>. This tag can be omitted.
   - Define a new tag <RoleDefinitions></RoleDefinitions>. This tag is a collection of several <RoleDefinition></RoleDefinition> tags. This tag stores information on SDM600 roles that are going to be mapped to a specific Windows User Group.
   - Define a new tag <Definition></Definition>. This tag is to specify available role definitions in SDM600. ABB SDM600 has two role definitions: ABB and IEC62351-8.
   - Define a new tag <Roles></Roles>. This tag is a collection of several <Role></Role> definitions. Each <Role> definition contains the Name and ID information.
   - In SDM600, the following roles' names and IDs are defined:

Role Definition	Name	ID
ABB	Administrator	-100
IEC62351-8	Viewer Operator Engineer Installer SECADM SECAUD RBACMNT	0 1 2 3 4 5 6

After modifying the *GroupRoleMappingStore.xml* file, remember to save the file and restart the following services:

- ABB Workgroup Management Service
- ABB Workgroup Replication Service
- pGina Service

8.2.6.5 Integrating Windows PC Events into SDM600 Windows Event Log Forwarder

SDM600 provides possibility to register security events from Windows PC. This functionality is independent from the ABB SDM600 Centralized Account Management for Windows PC and can be installed separately.

In order to enable ABB SDM600 Windows Event Log Forwarder follow steps below:

1. Add the Windows PC as a device in SDM600 (you can skip this step if it's already done for Centralized Account Management).
2. Select a device, for which the ABB SDM600 Windows Event Log Forwarder installer will be generated.

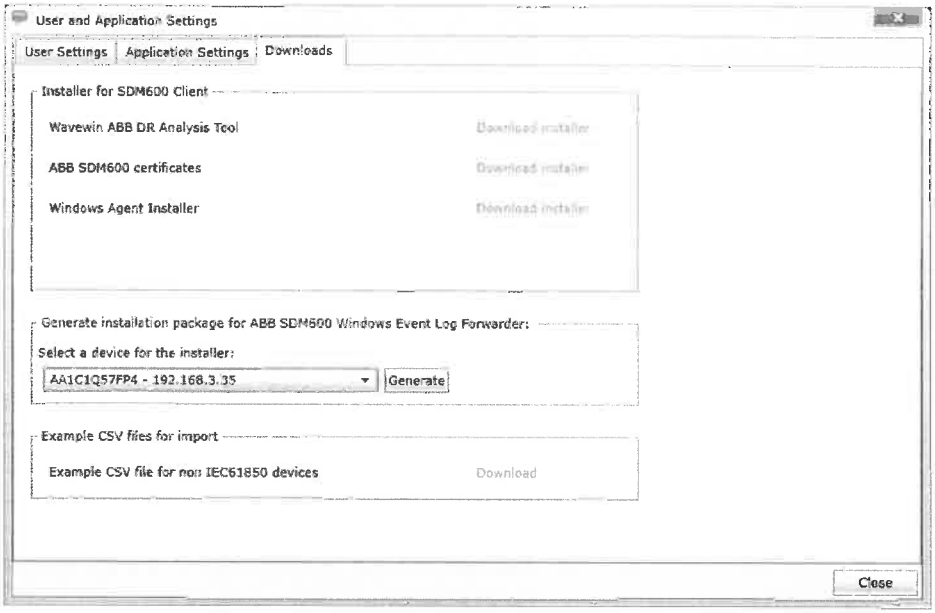


Figure 8.30: Generate WEF installer

3. Download installer on local computer by clicking **Generate** button.
4. Bring the file to the Windows PC on which the installer is to be installed.
5. Unzip the download package into a directory.
6. Run the installer.

The installer is tailored to this particular Windows PC. Installing the installer that is generated for another device will cause the ABB SDM600 Windows Event Log Forwarder to not work properly.

7. When the installation is completed, restart the Windows PC.

8.2.6.6 User Account Management

Setting up user accounts in SDM600 is a very important step. Best practices in cyber security recommend the principle of least privilege. The principle imposes on providing a user account with privileges that are essential to the user's work. Thus, it is

recommended to first set up proper user accounts with roles before starting to engineer SDM600.

SDM600 offers roles that are defined in the IEC 62351 standard. The roles and their definitions according to SDM600 are the following:

- *Viewer*: provides the assigned SDM600 user rights to view (read-only) available general interfaces in SDM600
- *Operator*: provides the assigned SDM600 user rights to operate the configured SDM600
- *Engineer*: provides the assigned SDM600 user rights to configure the SDM600 application (not included: security events and centralized account management)
- *Installer*: provides the assigned SDM600 user rights to configure SDM600 application (not included: security events and centralized account management)
- *SECADM*: provides the assigned SDM600 user rights to configure SDM600 centralized account management
- *SECAUD*: provides the assigned SDM600 user rights to configure SDM600 security events management
- *RBACMNT*: provides the assigned SDM600 user rights to configure the SDM600 Role to Right mapping
- *Administrator*: provides SDM600 user rights to perform user account administration and to configure SDM600.

A full definition of the IEC 62351 roles can be found in the standardization document. SDM600 redefines the roles according to the SDM600 application. However, SDM600 provides a UI for the user to redefine the rights for each user role.

For managing users, a dedicated toolbar is provided.

Figure 8.31: Toolbar at User Management Tab

To add new user, click **New User**, and enter the required information.

Figure 8.32: SDM600 Configuration - Add New User

Each entry is validated. Failing to comply to the formatting standard will be alerted and sufficient information on proper formatting will be given.

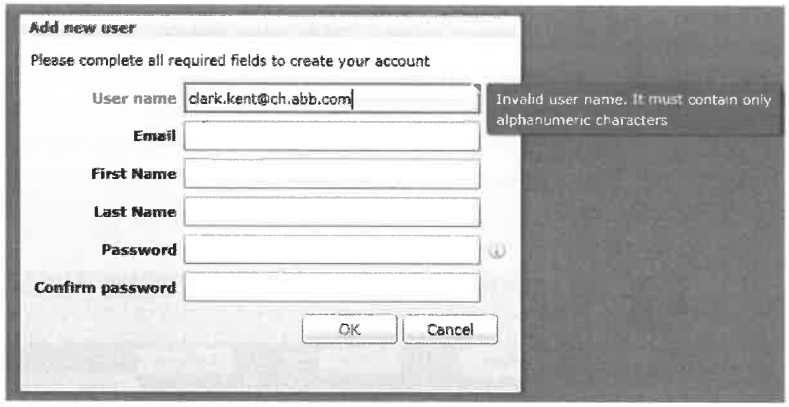


Figure 8.33: SDM600 Configuration - Add New User Format Check

SDM600 adopts a strong password requirement according to which, a password should have at least one special character, a number, a capital letter and a small letter. An example of a strong password is **J*p2leO4>F** (ref: *http://technet.microsoft.com/en-us/library/cc756109(v=ws.10).aspx*).

The password mentioned before is an example. Although it is a strong

password, it is not recommended to use that example as your password.

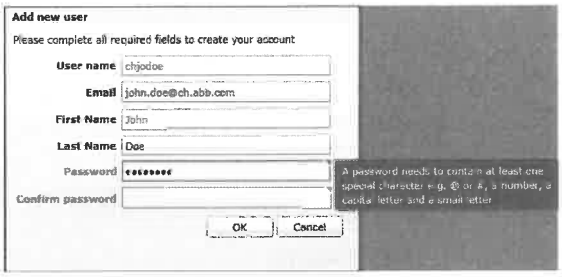


Figure 8.34: SDM600 Password Requirement

After registering a user, the administrator can assign roles to the user.

Figure 8.35: SDM600 Configuration - Assign Roles to User

For a new created user, the user has to immediately change their password on next login attempt.

To delete a user, select the user, then click **Delete user**.

If a user has forgotten their password, the administrator can help the user to reset the password. Select the user whose password is to be reset, then click **Reset password**. A new random password is automatically generated based on this request if the user confirms to reset the password.

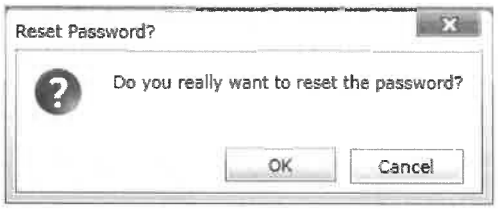


Figure 8.36: SDM600 - Confirm Password Reset for a User

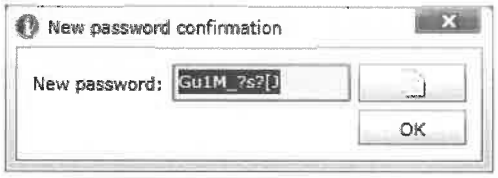


Figure 8.37: SDM600 User Password is Reset by Administrator

When the administrator resets a user's credentials, a pop up box with new credentials is shown. The credentials can be copied by pressing **Ctrl+C**. To paste the credentials, press **Ctrl+V**.

When the E-mail Notification feature is activated in SDM600, any change of a user's credentials is automatically forwarded to the respective user.

When a user's password is reset by the administrator, the user has to immediately change their password on next login attempt.

8.2.6.7 SDM600 Password Policy Settings

SDM600 provides the possibility to configure the policy for the user password. The following options are possible:

- Basic Settings
  - Enable or disable password must meet policy requirements
  - Minimum password length
  - Maximum password age
  - Expire warning
  - Password history enforcement
  - Number of maximum failed login attempts
  - Lockout duration

- Password Complexity Settings - a password must contain at least the following properties:
  - Lowercase characters (a - z)
  - Uppercase characters (A - Z)
  - Base digits (0 - 9)
  - Non-Alphanumeric

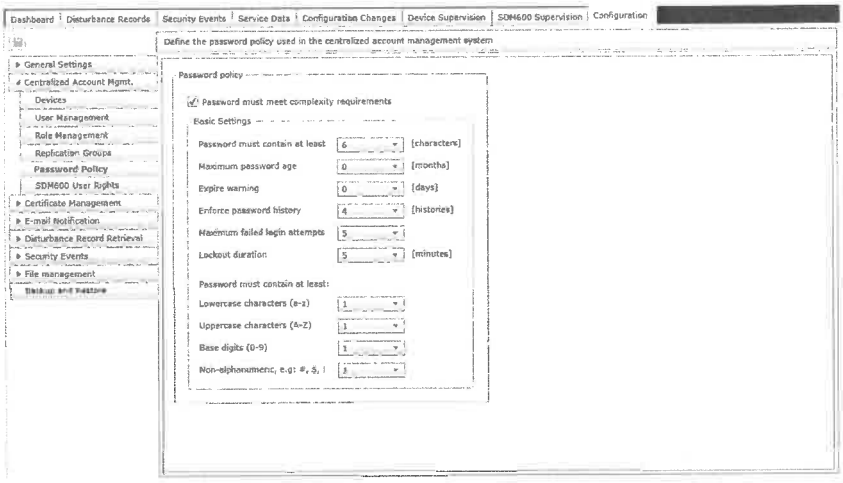


Figure 8.38: SDM600 Configuration - Password Policy Settings

8.2.6.8 SDM600 Role Management

SDM600 provides the possibility to configure the roles. As default, standard roles described in IEC62351 are configured. These roles cannot be modified or deleted.

In addition to IEC62351 roles, there is possiblity to create custom roles.

Follow below steps in order to create custom role

1. click on **New role...** icon
2. Fill required information

According to IEC62351, custom roles have negative Id values

If at least one custom role has been created, then additional icons are activated

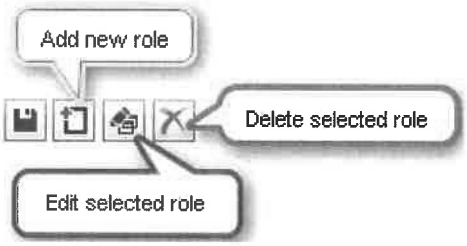


Figure 8.39: Custom roles icons

8.2.6.9 Replication Groups

It is possible to define groups of users, which will be replicated to the device. This functionality helps to save device memeory and decrease replication time

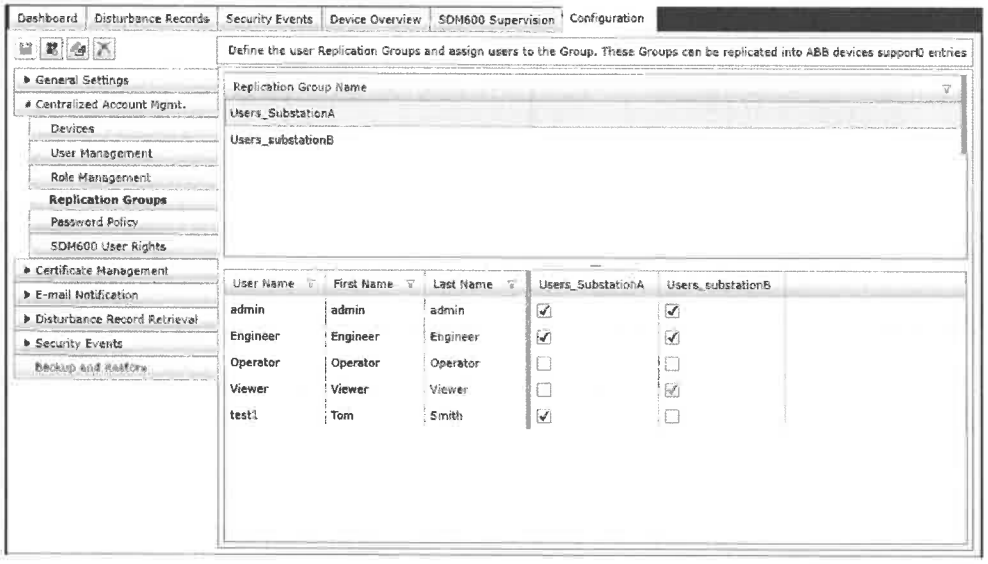


Figure 8.40: Replication groups

8.2.6.10 SDM600 User Rights

SDM600 provides the possibility for an authorized user to configure the role to right mappings for the SDM600 application. This flexibility allows end users to adjust the role to right mapping according to their policy. The standard role to right mapping that is recommended by SDM600 can be seen in the following figure.

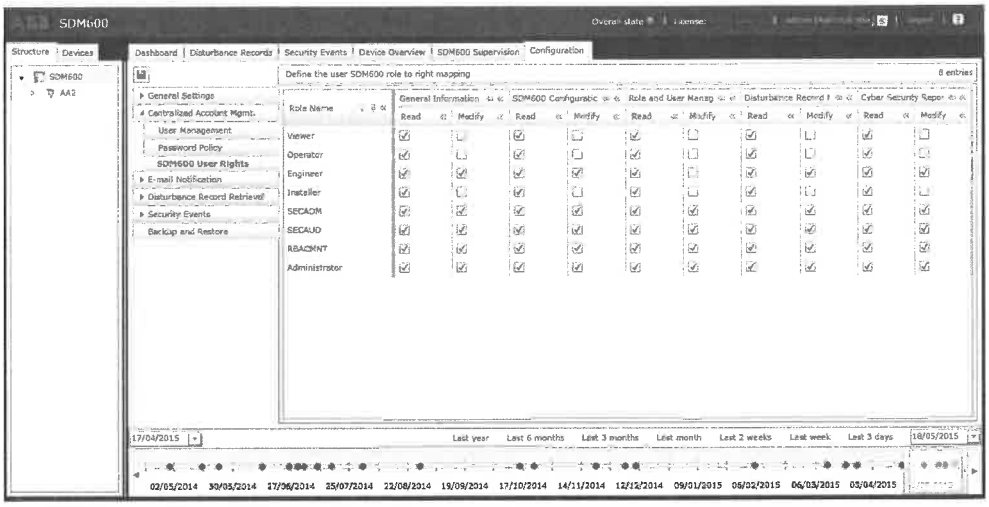


Figure 8.41: SDM600 User Role to Rights Mapping

To change the SDM600 role to right mapping, the authorized user can check and uncheck the read and modify checkboxes in **Configuration > SDM600 User Rights** on the role and on different parts of the SDM600 application.

From the role to rights perspective, SDM600 is divided into five parts:

- General Information
- Engineering of the SDM600 application
- User and role management
- Disturbance record settings and monitoring
- Security event[setting and reporting

8.2.7 Certificate Management

This feature enables SDM600 to modify default certificates settings, manage root certificate and generate device certificate for general purposes.

The information mentioned in this section should be edited with care. Misconfiguration on the certificate properties may cause SDM600 to stop work.

Settings in Certificate Management tab are affecting all certificates generated by the SDM600 (including CAM certificates). Increasing default certificate key length may impact device performance.

The Certificate Management setting provides the following functions to the user:

- Root certificate handling - allows user to import root certificates obtained from external certificate authority, regenerate self-signed root certificate and export CA private key to the file.

Keep CA private key file in safe place. Unauthorised use of private key can compromise SDM600 security.

- Default certificates creation values - enables to set default values for key length, validity date and exteneded attributes for newly created certificates.

Key length and validity date can be adjusted on certificate creation dialog.

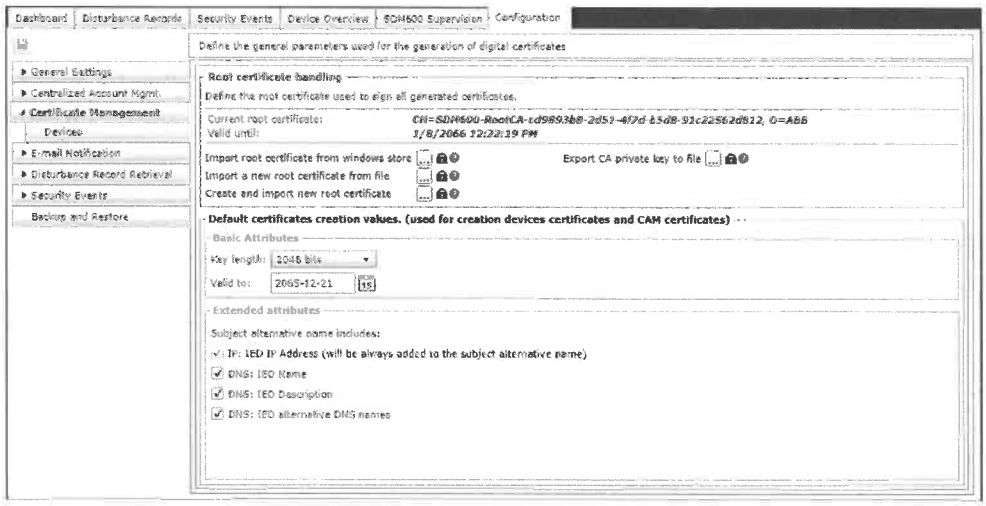


Figure 8.42: Certificte Management settings

8.2.7.1 Setting up Device certificates

SDM600 can generate general purposes certificate for every device defined in the structure. These certificates can be used for securing web connection or file transfer (if connected device is offering this funtion).

In order to generate certificate for device, follow steps below:

1. Navigate to **Configuration > Certificate Management> Devices** subtab.
2. Select one or more device.
3. Click on **Add new certificate** button.

Figure 8.43: Add new certificate button

4. Define certificate key length, validity dates and certificate password.

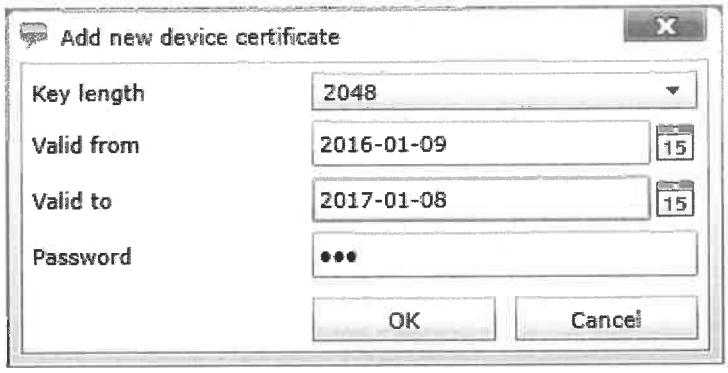


Figure 8.44: Certificate creation window

If certificates are generated for multiple devices in one step, then password for generated certificates will be the same.

5. Save newly created CAM package by hitting **Save** icon.
6. Copy certificate for selected device or devices.

It is possible to edit certificate properties by double click on device list. When chanages are done, it's necessary to click on **Save** icon.

8.3 User-Specific Configuration

SDM600 makes it possible for each user to define their own preference settings in the UI. To access this possibility, click the setting icon next to the username at the top right of the SDM600 UI. In User and Application Settings, the following tasks can be done:

- Update User Settings
  - Change user relevant information such as password, email address, first name and last name.

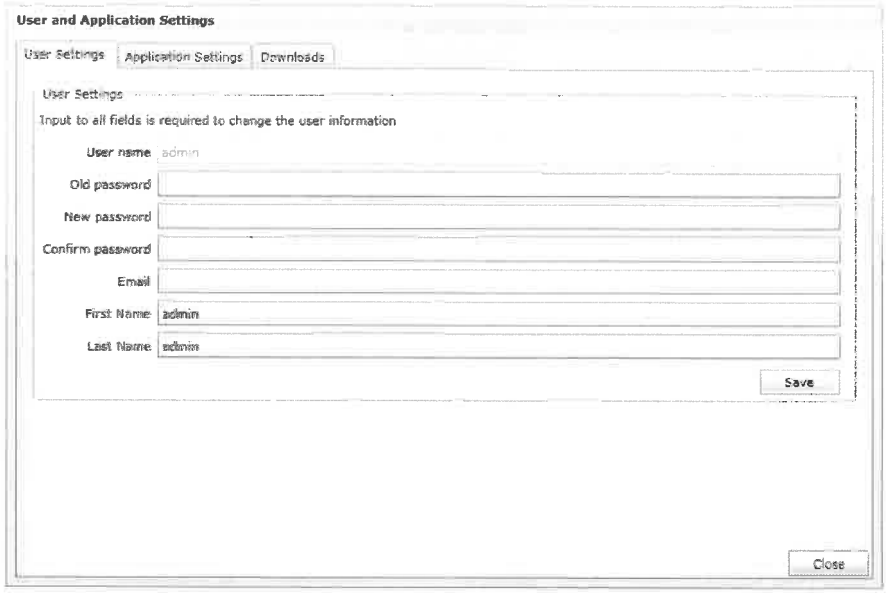


Figure 8.45: SDM600 User and Application Settings - User Settings

- Configure Application Settings
  - Dashboard time window duration: used to define the width of the dashboard time navigator. By default, the 1 month value is set. It is possible to set up a maximum of 13 months. Thus, it is possible to evaluate the current events and compare them to the same time last year.
  - DR analysis tool: used to define the preferred tool for analyzing a disturbance record entry

To specify the preferred DR analysis tool, the executable file of the tool has to be selected. The executable file has to be available on the PC from where SDM600 is accessed. In addition, the executable file should be able to take the disturbance record file as its first argument.

  - Name or Description shown in the Navigation Reference area: it is possible to show either the name or the description of the devices
  - Reset to the default SDM600 display settings: used to reset the user's display setting. The setting is applied only after the next login.

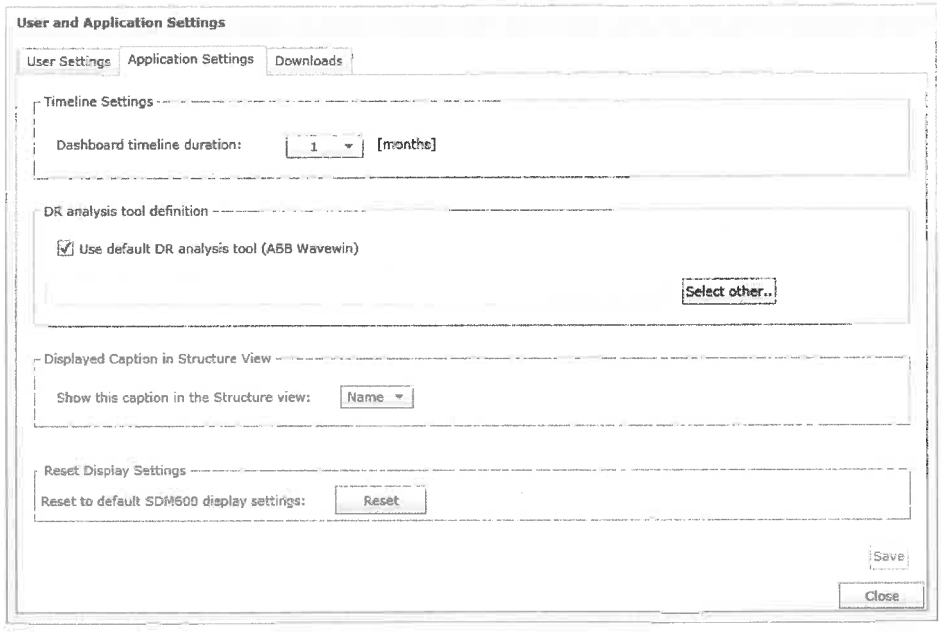


Figure 8.46: SDM600 User and Application Settings - Application Settings

- Get Downloadable Files:
  - Wavewin ABB - DR Analysis Tool
  - ABB SDM600 Certificates - for HTTPS connection
  - Windows Agent Installer - script working on Windows PC for collecting configuration information.
  - ABB SDM600 Windows Event Forwarder
  - Example of CSV file for importing non IEC61850 devices.

To download the ABB SDM600 Windows Event Forwarder and the ABB SDM600 Centralized Account Management to a Windows PC, the user needs to specify the IP address where these applications are to be installed. In addition, to download the ABB SDM600 Centralized Account Management to a Windows PC, the user needs to select the operating system version. When all the necessary information is selected, SDM600 generate the installer package. The user can then extract the installer package in a directory and run the installer.

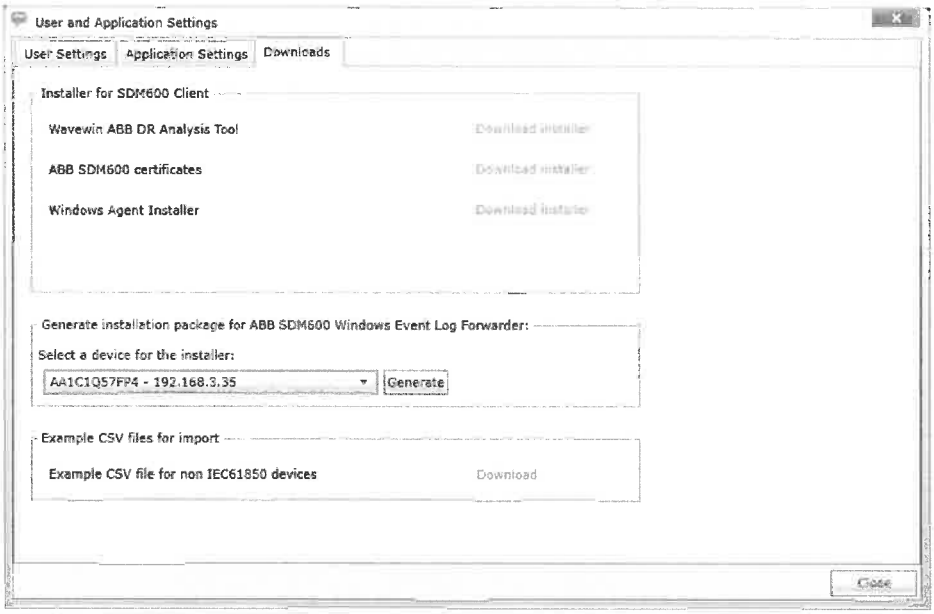


Figure 8.47: SDM600 User and Application Settings - Downloads

9 E-mail Notification

SDM600 provides the possibility to send e-mail notifications to users on the following events:

- A new user is created. When this option is activated, an e-mail is sent to the e-mail address of the user. The e-mail contains a notification that a user on SDM600 has been created. In addition, the initial password is sent in the e-mail.

  New users have to change their password when they access SDM600 for the first time.

- Administrator changes the user's password. When this option is activated, whenever the administrator of the SDM600 changes a user's password, an e-mail is sent to the user's e-mail address, informing the user of a new password.
- Disturbance record arrives in SDM600. When this option is activated, SDM600 sends an e-mail notification to pre-selected users in SDM600. SDM600 provides two variants of e-mail notifications when a new disturbance record arrives in SDM600:
  - Plain e-mail notification that informs the user of the arrival of a new disturbance record.
  - E-mail notification that informs the user of the arrival of a new disturbance record and also includes the corresponding PDF short report.
  - The user has the possibility to customize condition of the e-mail notification for disturbance record.

  Figure: condition editor for the email
- Information about certificate expiration. It's possible to configure how many days before certificate expiration SDM600 should inform defined users.

To set up the e-mail sending function, a user has to navigate to **Configuration > E-mail Notification**.

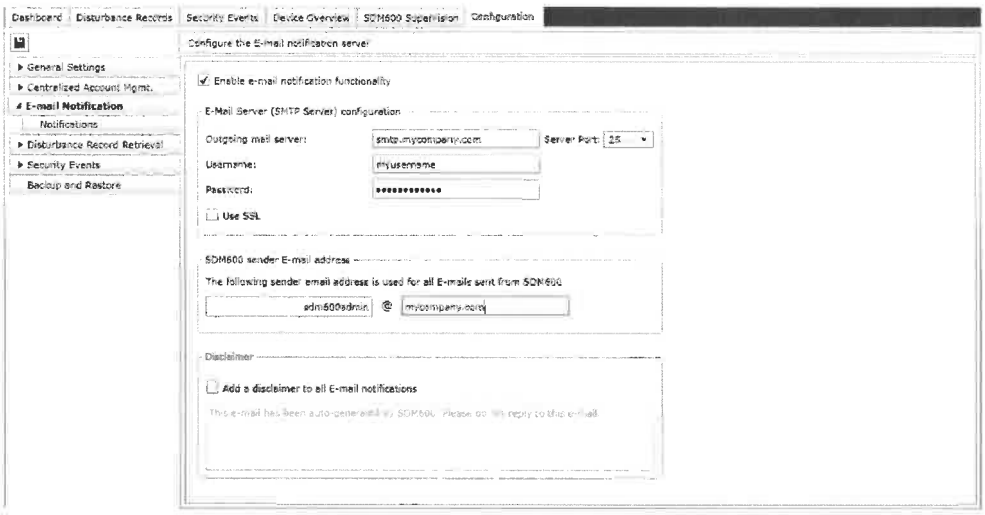


Figure 9.1: Setup of SDM600 E-mail Notification

The pre-filled information in the figure above is an example. You should enter proper information according to your SMTP server and account setup. Failure to enter the required information will cause the e-mail sending function to not work properly.

The following information is mandatory in order to setup the e-mail sending function:

- the address of a separate and running SMTP server for e-mail sending, such as *smtp.yourdomain.com*
- an SMTP username (some servers require full address like *username@yourdomain.com* in order to be able to send emails)
- an SMTP password
- the SMTP port number, normally port 25, 465 or 587 is used
- how to access the SMTP server: secure (via SSL/TLS) or non-secure
- the e-mail address of the sender (this needs to be a valid e-mail address)

It is mandatory to fill in all the required fields in this configuration setting.

SDM600 does not come with its own SMTP Server. In general, a user can set up their own SMTP server or it is provided by the internet service provider. For information on an SMTP server that you can use and the relevant information (such as address and port numbers), please consult your IT department.

To use the SDM600 E-mail function, the following conditions have to be fulfilled:

- Ensure that there is an SMTP server in your organization that can be used to send e-mail.
- Ensure that your firewall does not block the SMTP server traffic (normally port 25 is used).

After entering the SMTP configuration, the e-mail notification can be activated for different events.

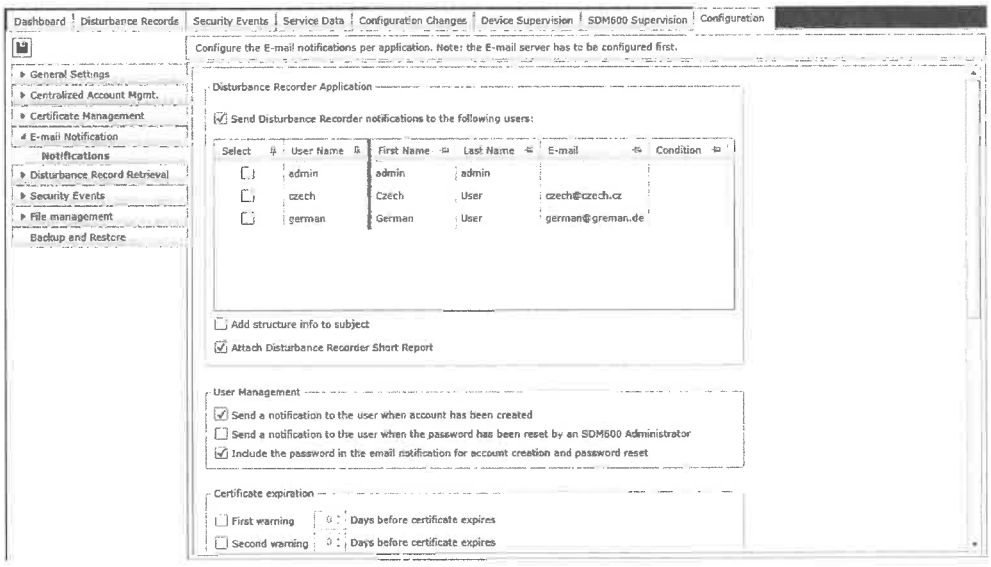


Figure 9.2: SDM600 E-Mail Notification

In SDM600 there are several notification available:

- Disturbance Recorder notification - allows to send email to defined users, when Disturbance Record is received by theSDM600.

Figure 9.3: Disturbance Recorder notification

When Disturbance Recorder notification is enabled as well as user to whom notification will be send, then option for defining email condition is enabled. In order to define email condition, click on **Add** link in Condition column. New window will appear.

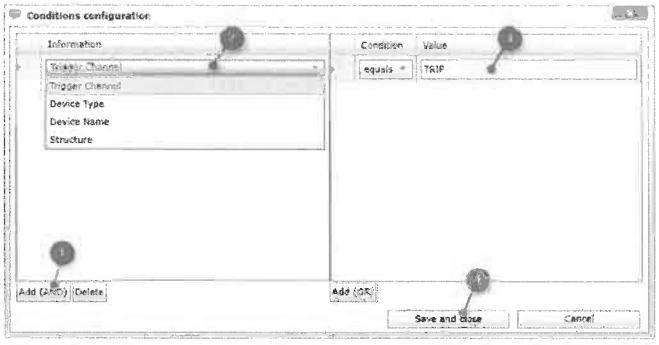


Figure 9.4: DR email condition editor

Click on **Add (AND)** button (1), select property form the list (2), define value (3). It is possible to add another value to the current property, by clicking on **Add (OR)** button, or define rule for another property by clicking on **Add (AND)** button (1). When email condition is ready, click on **Save and close** button (4).

- User management notification - allows to send email when account has been created or password has been reset by administrator to particular user. SDM600 can include password in the email for account creation and password reset.
- Certificate expiration - allows to send notification emails when SDM600 certificate is about to expire. It is possible to set two notifications periods and select users who shall receive notification.

Figure 9.5: Certificate expiration notification

- Statistics notification - allows to send daily/weekly/monthly statistics email to selected user. Statistics consist number of Disturbance Records, security events, configuration changes and user account changes within selected time range.

10 Disturbance Record Retrieval

SDM600 provides an automatic mechanism that periodically collects disturbance record data from selected devices. SDM600 automatically detects and transfers new disturbance records from selected IEDs and stores the disturbance data files in a designated database following the structure of the engineered network or substation topology.

10.1 Setting Up DR Retrieval Functionalities in SDM600

DR Retrieval in SDM600 is controlled with licenses. When a proper license is available, the user is able to set up SDM600 to collect disturbance records.

To set up the DR Retrieval function, do the following:

1. Navigate to **Configuration Tab > DR Retrieval** subtab
2. Configure the Disturbance Record Retrieval application settings, i.e:
   - Customize file name of the exported disturbance records files. There are three types of the file naming: Original file name, Filename structure according to the COMNAME standard and custom setting.
     Custom file name can be configured by using of predefined parts (like DR Trigger time, Company Name, etc.)

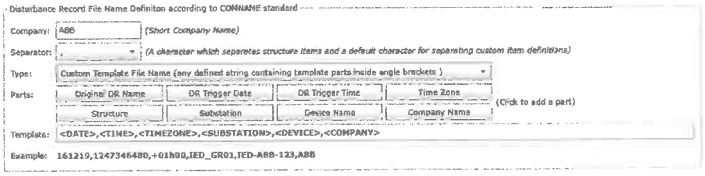


Figure 10.1: Disturbance Record File Name Definition

   - Automatically generate PDF Short Report when a disturbance record arrives to SDM600. To enable this function, navigate to **Configuration tab > Disturbance Record Retrieval**, and then check the **Automatically generate short reports when a new disturbance record is retrieved** option.

     Generating of the short report is resource consuming operation, hence is recommended to not select this function on heavly loaded systems and generate report on demand instead.

   - Automatically save disturbance record files to the SDM600 server folder structure when a disturbance record arrives to SDM600. To enable this function, navigate to **Configuration tab > Disturbance Record Retrieval**, and then check the **Save new DR files to file system** option.

It is important to define a directory at the SDM600 server where such disturbance record files are to be saved. The directory structure can be defined in the provided text box. See Figure. When no specific directory is defined, SDM600 will store it directly under the installation directory *<Installation directory> \ClientBin\Download\DR*. For example, in Windows 7 x64 OS, it is stored under *C:\Program Files (x86)\ABB\SDM600\ClientBin\Download\DR*.

- Export collected disturbance records to the SDM600 server folder structure. To execute this function, provide the directory to store the exported DR files, then click **Export all DRs**.

It is important to define a directory at the SDM600 server where such disturbance record files are to be exported. The directory structure can be defined in the provided text box. See Figure. When no specific directory is defined, SDM600 will store it directly under the installation directory *<Installation directory> \ClientBin\Download\DR*. For example, in Windows 7 x64 OS, it is stored under *C:\Program Files (x86)\ABB\SDM600\ClientBin\Download\DR*.

After entering the directory into the text box for directory definition, remember to save the changes to ensure that SDM600 takes this directory into account while exporting the collected disturbance records files.

Figure 10.2: SDM600 DR Retrieval Configuration - Application Settings

3. To configure further the devices for disturbance record collection purposes, navigate to subtab **Devices**. This subtab shows the list of available devices based on the selection on the navigation reference area. To start collecting disturbance records from a particular device, start by clicking on the checkbox at the Active column to activate the devices.

By default, SDM600 activates the IEDs for disturbance record collection if there is still a license available.

To select multiple entries of IEDs for DR Retrieval activation, select the rows. Next, right-click with the mouse and select **Activate Selected IEDs** from the context menu. To deactivate the entries, select **Deactivate Selected IEDs** from the context menu.

Activating the DR Retrieval of an IED imposes on SDM600 to start collecting disturbance records from the IED. Deactivating the DR Retrieval of an IED will cause SDM600 to delete the collected DR files.

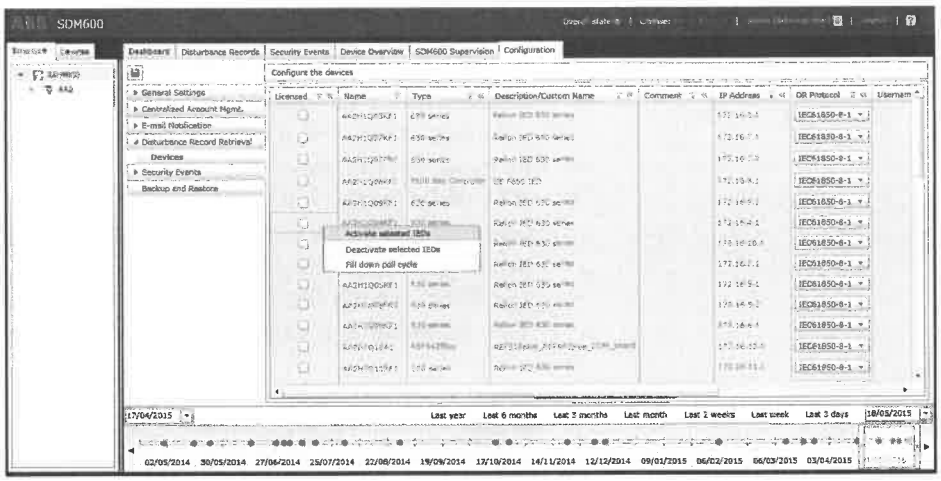


Figure 10.3: SDM600 DR Retrieval Configuration - All Selected IEDs are Activated

4. By default, SDM600 communicates with the devices using IEC 61850-8-1 protocol (MMS protocol). However, SDM600 also supports devices that do not communicate using IEC 61850-8-1. In this case, FTP protocol can be used. Moreover, SDM600 also supports the possibility to read the disturbance records that are stored manually by user on a specific harddisk/drive or network drive. To configure such communication options, navigate on the device entry on the Devices subtab and modify the following columns accordingly:

   - **DR Protocol**: select a suitable protocol to be used to communicate with SDM600 for disturbance record retrieval. Available ways of communication are IEC 61850-8-1, FTP and Directory.
     - IEC 61850-8-1 : DR files of devices are collected by SDM600 by using IEC 61850-8-1 MMS protocol.

- FTP : DR files of devices are collected by SDM600 by using standard File Transfer Protocol.
- Directory : This method is used when DR files are collected manually by user and placed into a folder in a computer where SDM600 is installed or in a folder of another computer which is accessible by SDM600. In this case, SDM600 reads the specified folder and imports the DR files into SDM600.
- RTU Web API : This method is used when DR files are collected from the RTU500 device. SDM600 can collect COMTRADE files from RTU using IEC 61850-8-1 as well as IEC 60870-5-103 protocol. DR file format is recognized automatically and suitable converter is used if needed.

FTP protocol and Directory method of collecting DR files are normally used for devices that do not support IEC 61850-8-1 protocol.

- **Username**: if FTP or RTU Web API protocol is chosen as a way of communication, it is important to enter the respective username to access the FTP directory of the device.
- **Password**: if FTP or RTU Web API protocol is chosen as a way of communication, it is important to enter the respective password to access the FTP directory of the device.
- **RTU Role Name**: if RTU Web API protocol is chosen as a way of communication, it's important to enter the name of the role with defined privileges to read disturbance record files on the RTU device.
- **DR Path**: specify the directory where the disturbance record files are located. This information is valid for all types of communication.

If selected DR Protocol to collect the DR Files is set to Directory, it is important to specify correctly the DR Path. There are two possible variants:

- If the directory where the DR files is located is on the same computer as the SDM600, simply fill in the DR Path with the path to the directory. For example, if the DR files are located under *C:\Substation_Baden\Bay1\IED1*, then simply type in *C:\Substation_Baden\Bay1\IED1* into DR Path column of the respective IED.

Figure 10.4: Example of DR Path Entry Where DR Files Are on The Same Computer as SDM600

- If the directory where DR files are stored is located at a different computer, it is important to make sure that the directory is accessible from SDM600, i.e. by sharing the folder. While sharing the folder, it is important to ensure that the SDM600 service that handles this function (ABB SDM600 IED Communication Service) is running under an account which has enough privileges to access the network path or the remote shared folder, i.e. same credentials, same right as used on the other computer that stores the DR files.
  Next, fill in the DR Path with the full UNC path (\\computername\sharedfolder). For example, if the DR files are located under a computer with IP address 10.41.141.107 at C:\Substation Baden\Baden\IED2\ drive, and C:\Substation Baden is a shared folder, the correct way to write the full UNC path is **\\10.41.140.107\Substation Baden\Baden\IED2**

Figure 10.5: Example of DR Path Entry Where DR Files Are on Another Computer

In general, when there is a need to access files that are located on another computer, it is common to map the network drive to the local drive. In SDM600 DR collection mechanism, this will not work. It is important that only the full UNC path to the folder on another machine is given to SDM600.

In the case where the particular SDM600 service seems to run under an account which does not have enough privileges to access the shared folder, do the following steps:

- Navigate to **Windows Start menu** and type in **Services**, then select and click on **View Local Services**.

- Right click on **ABB SDM600 IED Communication Service**, and click on **Stop** to stop the service.

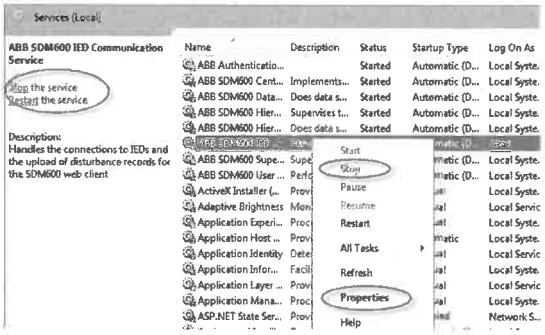


Figure 10.6: Windows Services - Navigate To ABB SDM600 IED Communication Service's Control and Properties

- Click on **Properties**, and navigate to the **Log On** tab.
- Click on **This Account** and then fill in the username and password for the account with proper privileges. It is important to ensure that this particular user has local administrator privileges. Note that the account in the following Figure is an example.

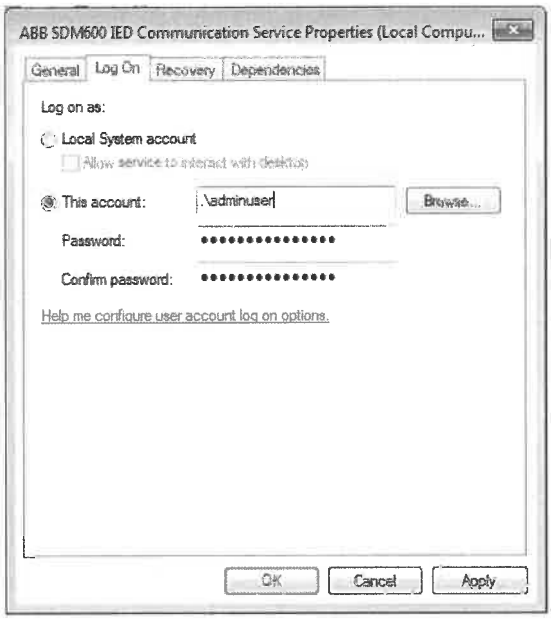


Figure 10.7: ABB SDM600 IED Communication Service Properties - Log On User

- Click **OK** to conclude the changes.
- Right click again on the **ABB SDM600 IED Communication Service**, and click on **Start** to start the service.

This case can be identified by checking whether it is possible to map the same shared folder on Windows Explorer. If mapping the same shared folder on Windows Explorer is possible, but SDM600 is not able to access the shared folder, this is an indication that due to certain setup in Windows OS, the SDM600 service is running under an account that has not enough privilege to access the shared folder.

5. By default, SDM600 polls the disturbance record every 60 seconds. To adjust the polling frequency, navigate to the **Configuration > General Settings > Device Settings > Poll Cycle (sec)** column and enter the value in seconds.
6. Click **Save** to commit the changes.

10.2 Analyzing Disturbance Records in SDM600

In order to analyze DR files in SDM600, follow the steps below:

- Select a DR entry on the SDM600 Dashboard

- Next, double click the DR point. This action brings the user to the particular DR entry that is selected on the dashboard.

Figure 10.8: SDM600 DR Analysis - Dashboard

Figure 10.9: Clicked DR on SDM600 Dashboard is Highlighted in DR Tab

- After that, user can analyze the DR by performing one of the following actions:
  - Download the DR files (in zip file)
  - Analyze the DR by using external analysis tool - Wavewin ABB launches automatically and shows the analyzed data or other user-defined third party analysis tool

    SDM600 allows to analyse multiple DRs at one time or merge them in ABB Wavewin. In order to open multiple DRs, select them on the list and click on *Evaluate* icon on the toolbar.

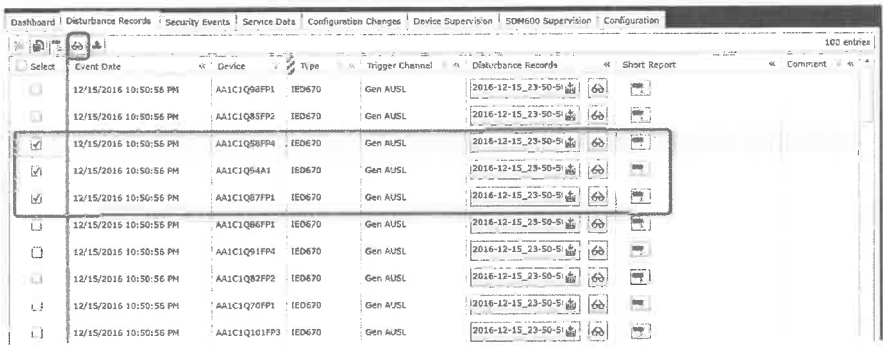


Figure 10.10: Disturbance Record files merge

SDM600 provides the possibility to analyze the incoming disturbance record using a user-defined 3rd party analysis tool. To define this, navigate to User and Application Settings at the top right corner of the page. Simply click on the username. Next, navigate to the Application Settings tab and then focus on the DR analysis tool definition area. After this, the user has to specify the link to the executable file.

In order for the user-defined third party DR analysis tool to work, the tool executable should be able to take the disturbance record file name as the first argument of the executable.

- Download the DR Short Report (in pdf format)

When the DR Short Report button is pressed, respective DR Short Report is generated and automatically launched in the new tab. It is possible that a browser disables pop-up windows by default. Different browsers behave differently. To enable pop-up windows on the browser, refer to the user manual of the browser.

Information regarding the Wavewin ABB application installer is available in the document 1MRS757749 - SDM600 Installation Guide - SDM600 Client Side Installation.

11 Security Events Settings

SDM600 offers the possibility to collect security events or logs that are sent in the format of Syslog from devices and applications. Additionally, SDM600 can also forward all events to another Syslog aggregator.

Security events in SDM600 are:

- Events that are caused by user actions in the system under SDM600.
- Events related to security issues from operating systems and security software (such as Anti-virus) of the system under SDM600.

Syslog is a standardized way for logging in computer systems. It is standardized by the IETF in RFC 5424. In most cases, the Syslog data is sent in clear text, unless the communication protocol is secured by means of encryption (for example, by using SSL). Unless the device is designed to connect to SDM600 securely, SDM600 receives the Syslog message in the clear text format.

Setting Up Security Events Collection in SDM600

In order for SDM600 to receive security events and store them completely in the SDM600 system, the following steps have to be executed:

- The devices that send Syslog events or the computers where an application sends out Syslog events have to be registered as devices in SDM600. To register a device, navigate to **Configuration > Structure**.
- Activate the devices in SDM600 for centralized activity logging so that SDM600 stores the events.

To activate devices for centralized activity logging, navigate to **Configuration > Security Events**. Activate the devices which need to send Syslog events. Remember to save the changes.

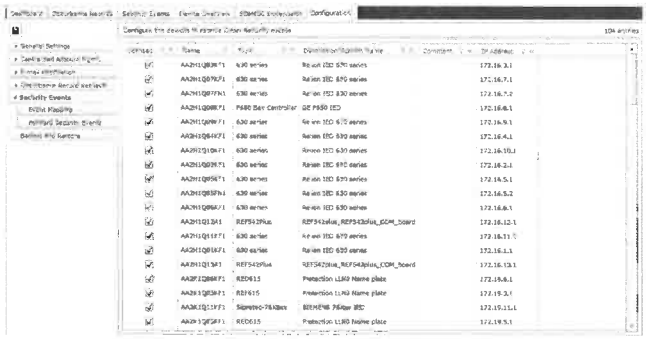


Figure 11.1: Activation of Devices for Security Events Purpose

SDM600 does not store events that arrive to SDM600 if the sender is not registered in SDM600. SDM600 only shows the 100 latest events.

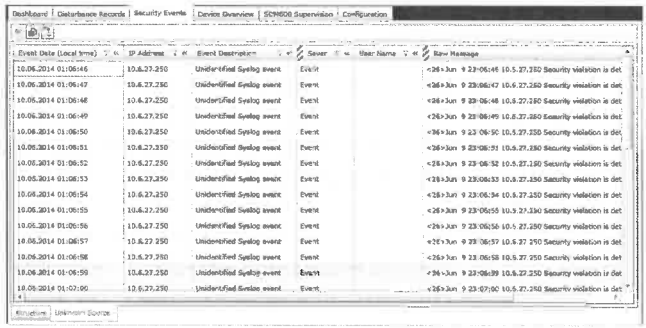


Figure 11.2: SDM600 Security Events - Unknown Source

When SDM600 receives Syslog events from devices that are activated, SDM600 tries to map the incoming events to the pre-defined available event type according to SDM600.

SDM600 provides numerous pre-defined event types. The pre-defined event types represent particular and relevant security events. In most cases, the pre-defined event types represent user activity events that are recognized by most industry cyber security standards. In SDM600, all user activities are cyber security relevant activities. Each SDM600 pre-defined event type has its own EventID and description. Examples of such pre-defined event types are:

EventID	Event Description
1110	Log-in successful
1115	Password expired, Log-in successful
1210	Log-out (user logged out)
1710	Device reset to factory default
2115	User account enabled successfully
2130	User creation failed

For a complete list of the available event types in SDM600 refer to Appendix A.

SDM600 provides a UI for the user to observe the incoming events. To view the incoming events and their event types, navigate to **Security Events tab.**

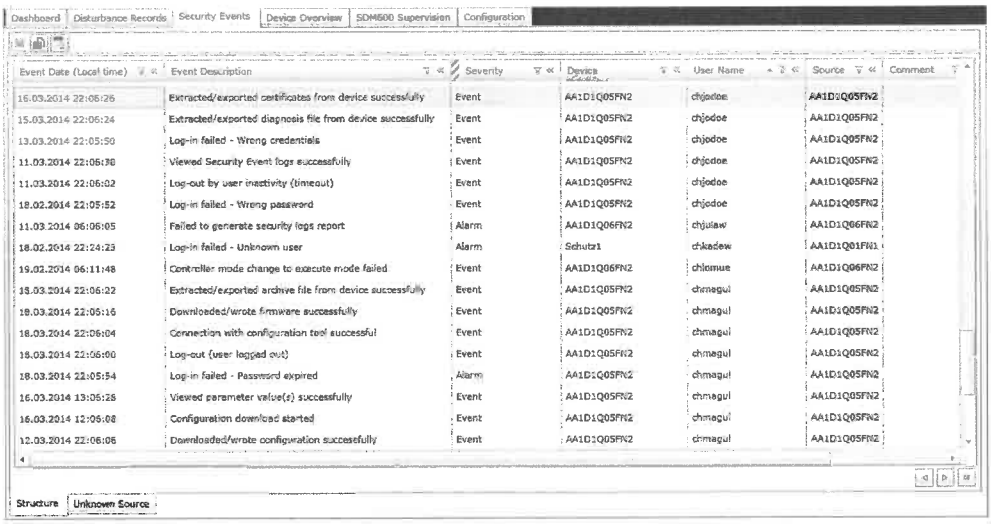


Figure 11.3: SDM600 Security Events Tab

If mapping cannot be done due to the fact that the Syslog event cannot be fully understood by SDM600, SDM600 categorizes the event as unknown event type (EventID 9990) and stores the event in SDM600 persistence. When the user knows more about the context of the unknown Syslog event, the user can re-categorize the unknown event type into a known event type by using the UI available inSDM600.

Map Unknown Event Type to Known Event Type

SDM600 provides an intuitive interface to map the unknown events to SDM600 known events. To conduct the mapping operation, navigate to **Configuration > Event Mappings**. In this part, all the events of unknown type (EventID 9990 and EventID 9991) are listed.

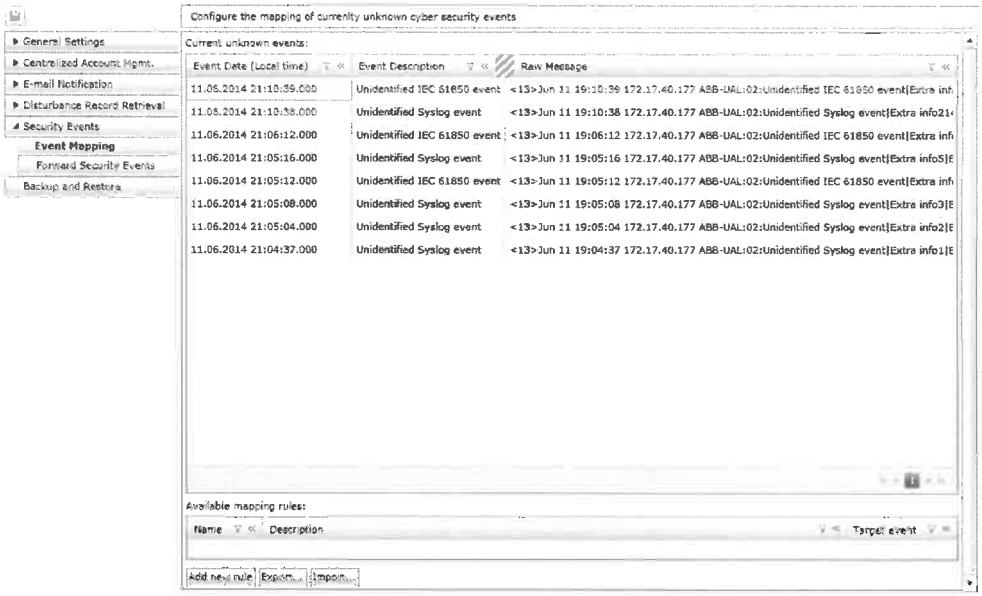


Figure 11.4: SDM600 Configuration - Event Mapping - List of Unknown Events

To start mapping the unknown events, do the following:

1. Click an unknown type security event for which a rule is to be created.
2. Click **Add New Rule**. A mapping rule creator window opens.
   Enter the necessary details, such as:
   - Name
   - Description
   - Rule conditions. This can be done by constructing conditions that the security events should meet.

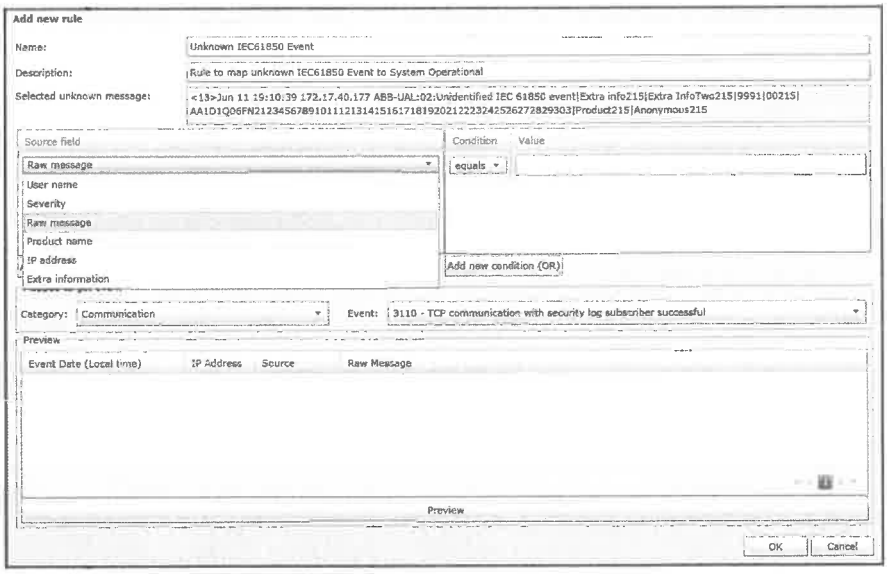


Figure 11.5: Create a New Mapping Rule for Unknown Event - Selecting Source Field

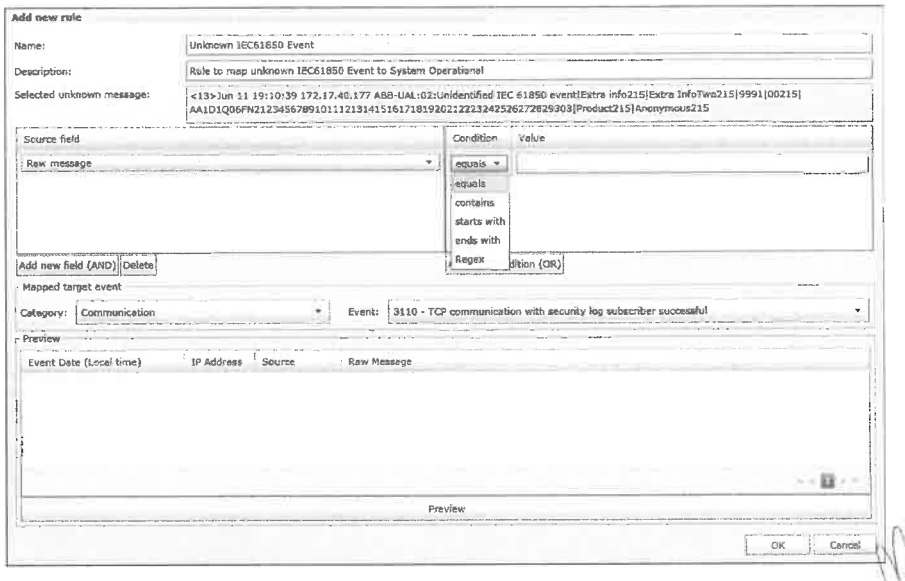


Figure 11.6: Create a New Mapping Rule for Unknown Event - Constructing Conditions

- New defined event type. After defining the rule conditions, it is important to select the new event type that is assigned to this kind of security events.

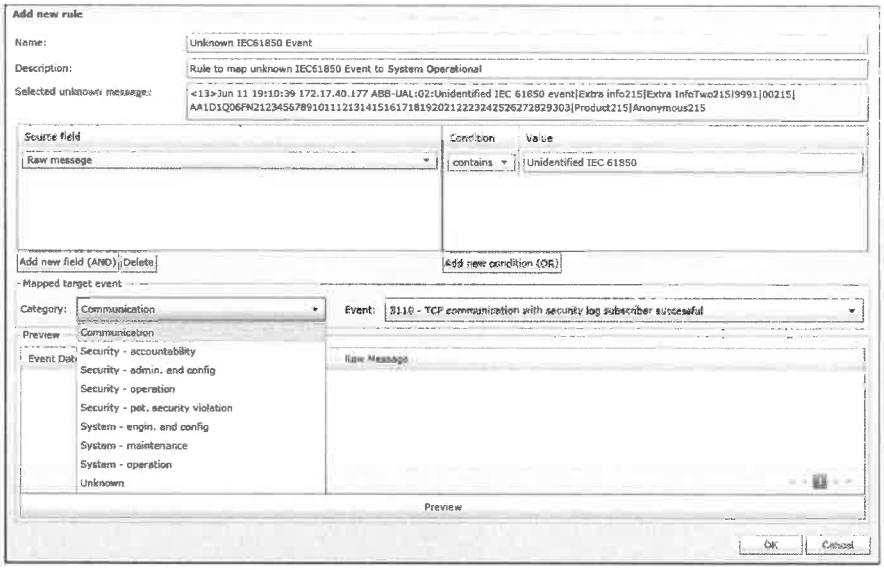


Figure 11.7: Create a New Mapping Rule for Unknown Event - Select Category to Map

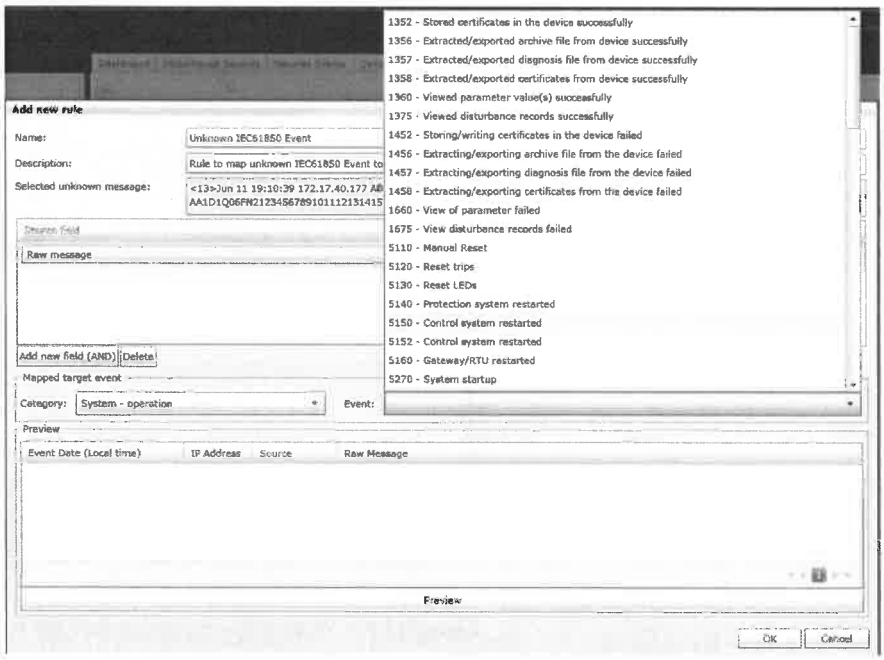


Figure 11.8: Create a New Mapping Rule for Unknown Event - Select Event Type

When a single rule is created, SDM600 tries to match all the available unknown types of security events to this rule.

- Before committing to the changes, a user can preview the affected security events by clicking **Preview**.

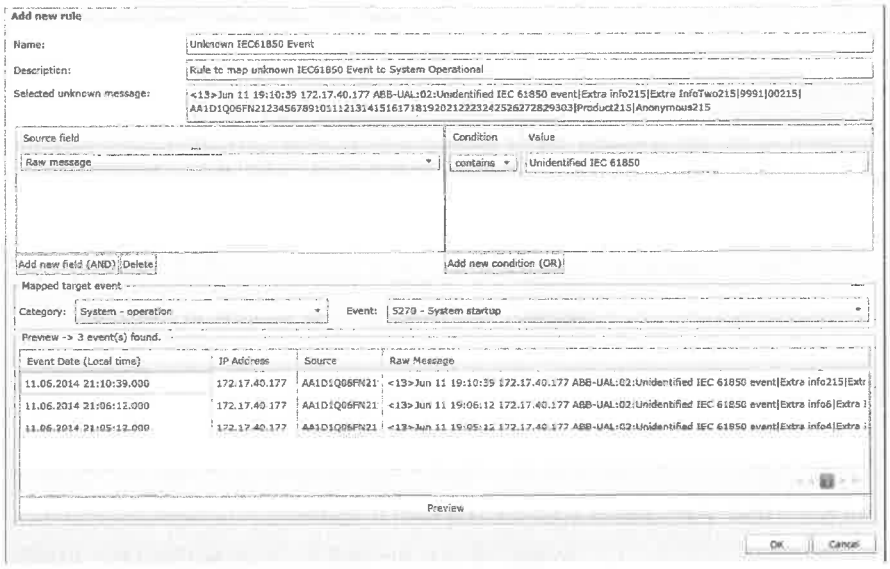


Figure 11.9: Previewing the Affected Security Events Based on the Newly Created Mapping Rule

3. To apply the changes, click **OK**. Once the rule is applied, SDM600 will map the unknown rules to the selected known event type and the newly mapped events will disappear from the list of unknown events.

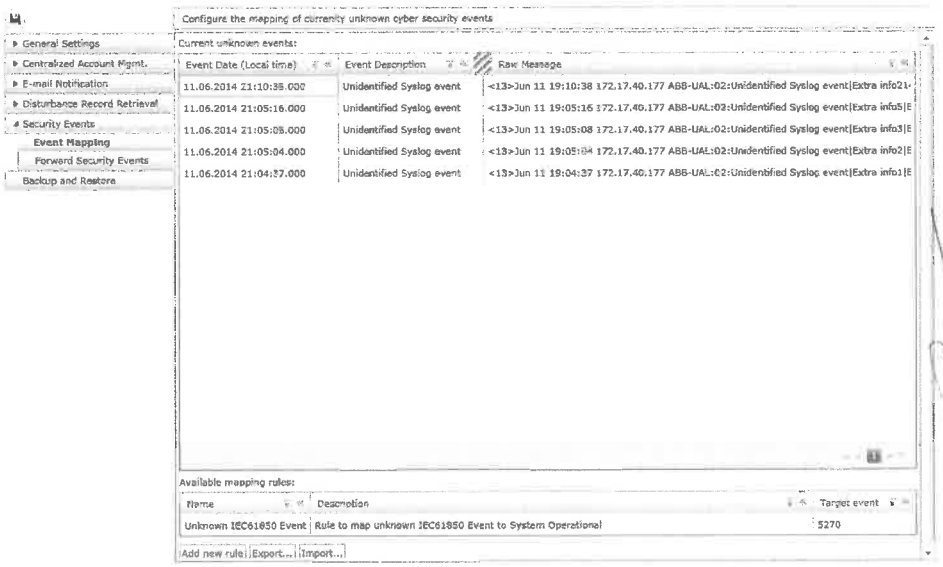


Figure 11.10: Newly Mapped Events are Removed from List of Unknown Events

SDM600 provides the ability to export the rules to a file. This is done for backup purpose or to apply the same rules on another SDM600 installation. To import the rules, click **Import Rules** and select the backup file.

Enabling Windows PC to Send Security Events to SDM600

As a Centralized Activity Logging unit, SDM600 provides a possibility for a Windows PC to send Windows security and application events to SDM600.

Windows security events are events that are generated during login/logout activity or other security-related events specified by the system's audit policy. By using a special SDM600 application – ABB SDM600 Windows Event Log Forwarder – SDM600 translates Windows Security Events log entries into SDM600 security events.

To enable this, the user has to download the installer to be installed on the Windows PC. This installer can be found in the **User and Application Settings > Downloads**. Follow the steps below:

1. To benefit from this feature, the Windows PC has to be registered as a device in the SDM600.
2. Download the ABB SDM600 Windows Event Forwarder and CAM Prerequisites and install it on the Windows PC.
3. Click **Generate Installation for ABB SDM600 Windows Event Log Forwarder for Windows PC**.
4. Click **Generate.**
5. Bring the file to the Windows PC on which the installer is to be installed.
6. Unzip the download package into a directory.
7. Run the installer.

The installer is tailored to this particular Windows PC. Installing installer that is generated for another device will cause the integration of the Windows PC to the ABB SDM600 Windows Event Log Forwarder to not work properly.

8. When the installation is completed, restart the Windows PC.
9. When the Windows PC is up and running, whenever there is a security event log entry that is triggered by the Microsoft Windows OS, the event is sent to SDM600.

It is important to regularly monitor the events that come to the SDM600 Centralized Activity Logging. Regular

monitoring makes it easier to detect anomalous behavior in the amount of received logs. When there is a wrong configuration in the Windows operating system, there is a chance that a Windows PC sends lots of events. In order not to fill in the SDM600 database with unnecessary events, it is possible to temporarily disable the installed ABB SDM600 Windows Event Log Forwarder on the Windows PC. To disable the ABB SDM600 Windows Event Log Forwarder on the Windows PC, do the following:

- Go to Start program in the Windows PC.
- Select *services.msc*, then press **Enter**.
- Find ABB SDM600 Windows Event Log Forwarder.
- Right-click on the service ABB SDM600 Windows Event Log Forwarder.
- Click **Stop**. By stopping the service, the ABB SDM600 Windows Event Log Forwarder stops forwarding any new Windows security events.
- To enable the service again, repeat the same steps, then click **Start**.

By default, SDM600 maps Windows Security Events to SDM600 specific events. The mapping table is available in the Appendix B.

Forwarding Incoming Security Events to Third Party Syslog Aggregator

It is also possible to forward incoming security events to another Syslog server or aggregator. To do so, navigate to **Configuration > Security events > Forward Security Events**. On the toolbar, click the button for Syslog Server Settings. Enter the required information for the external Syslog server. Remember to save the changes. When this external Syslog server is set up, any incoming security events are immediately forwarded to the external Syslog server.

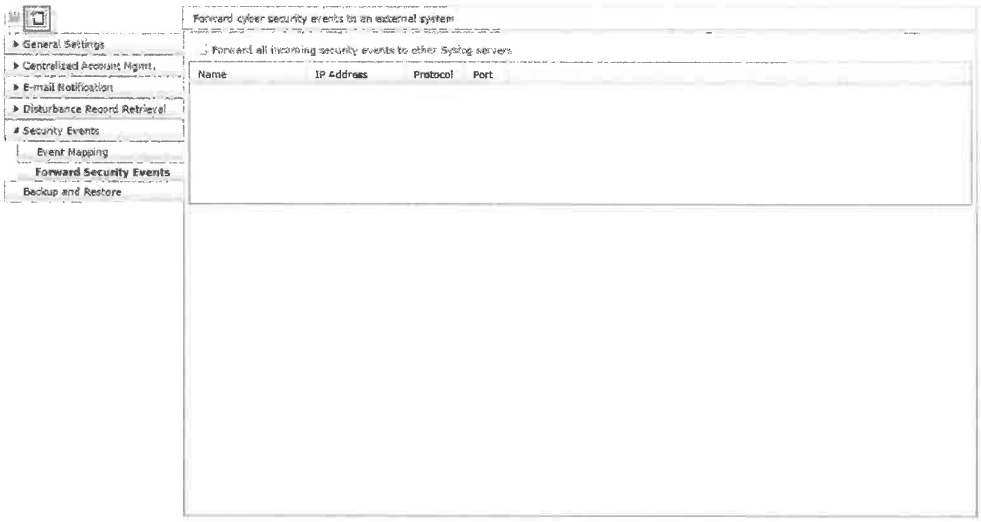


Figure 11.11: Registration of External Syslog Server - Button to Add External Syslog Server

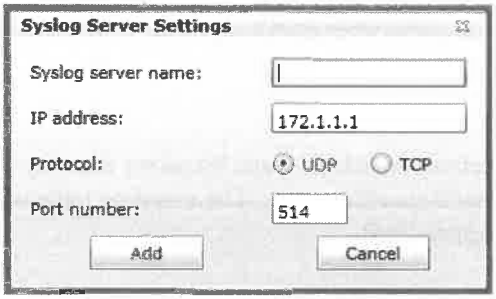


Figure 11.12: Registration of External Syslog Server - Enter Server Details

It is important to know that the Syslog events that are forwarded to the external Syslog server are not SDM600 processed Syslog events. The forwarded Syslog events are pure Syslog events that are received by SDM600. The events that are shown in the SDM600 UI are already processed by SDM600.

SDM600 Cyber Security Events

By default, SDM600 also sends out cyber security events when a user performs some actions. Most of the events are broadcast when the user makes configuration changes. SDM600 records information such as the username, time of the event, type of the event and some extra information regarding the action that triggered the event. SDM600 cyber security events are shown on the most upper part of SDM600 Dashboard.

Figure 11.13: SDM600 Cyber Security Events on Dashboard

To view SDM600 cyber security events in detail, navigate to Security Events tab. An SDM600 cyber security event can be indicated by its source, i.e. SDM600.

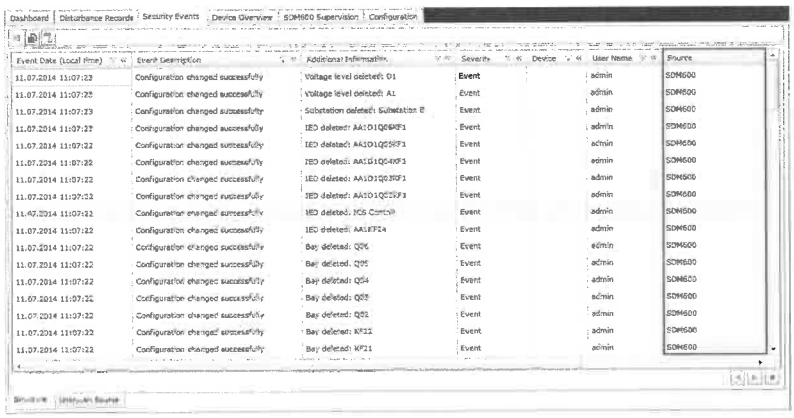


Figure 11.14: SDM600 Cyber Security Events in Security Events Tab

A list of SDM600 Cyber Security Events is available on Appendix C.

12 File Management

The SDM600 allows to store and manage device specific files like firmware and configuration. SDM600 is storing last five versions of the configuration and firmware files for each device.

Current release of SDM600 is supporting RTU500 rel. 12 family devices only.

In order to set up file management for the device navigate to **Configuration tab > File management** and configure following properties:

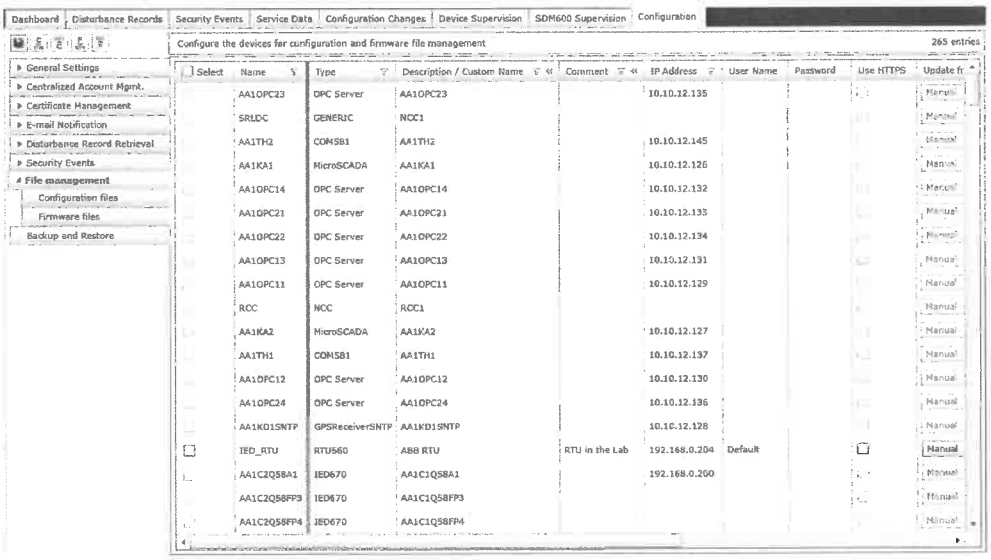


Figure 12.1: Device settings for file management

- Username - username for the account on the device
- Password - credentials of the account on the device
- Use HTTPS - securing connection with the device

Before using HTTPS option, make sure that SDM600 certificate for device is generated, uploaded to the device and properly configured.

- Firmware Role Name - Name of the role with configured red/write rights for device firmware
- Configuration Role Name - Name of the role with configured rights for updating device configuration

When new RTU device is added, SDM600 is configuring Firmware and Configuration Roles Names to default vaules. Make sure that user account used to connect with the RTU is assigned to these roles and propper righs are configured on RTU side. Otherwise change roles names accordingly.

All RTU related user accounts configured in the SDM600 have to have *Viewer* right in the RTU.

It's possible to schedule automatic backup of the device configuration. This option is configurable per device in the **Update Frequency** column.

After successful configuration, SDM600 allows to perform following operations:

Figure 12.2: File management icons

- Read configuration from the device
- Write configuration to the device - in the newly opened window, there is possibility to choose file from the disk or file already stored in the SDM600 database.

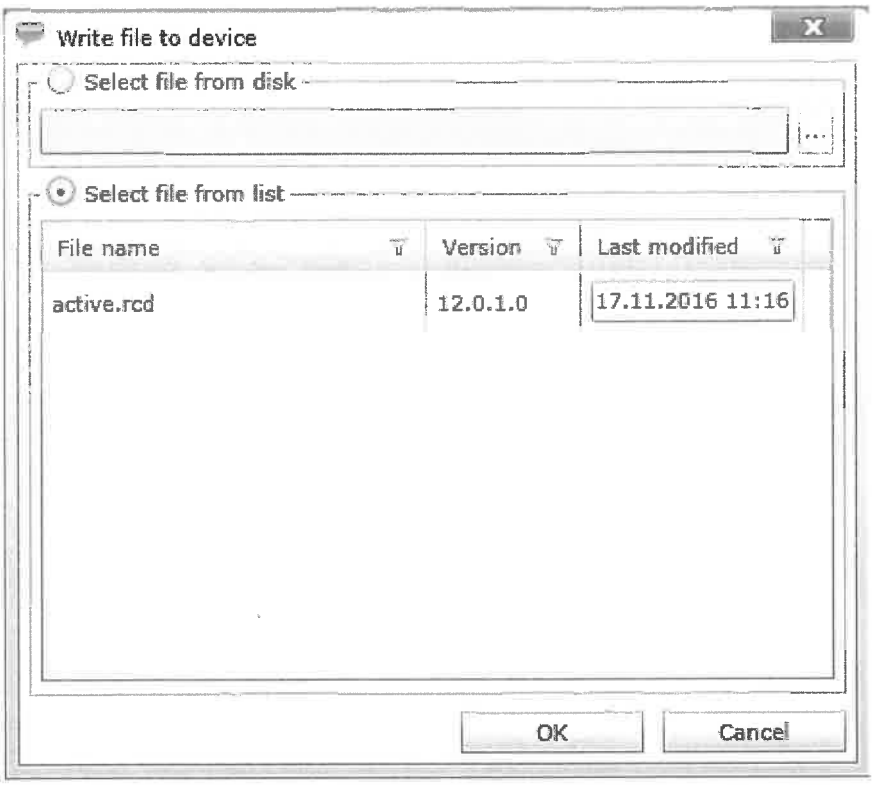


Figure 12.3: Write file to the device

After successful write, device is restarted and new configuration is activated.

- Read firmware from the device
- Write firmware to the device - this function is opening similar window as write configuration function.

On Configuration Files and Firmware Files tabs is a list of files currently stored in SDM600. There is also possibility to download these files to the drive.

In order to download configuration or firmware file to the drive,

1. navigate to corresponding sub tab in the File management tab
2. select device, from which file will be saved on the drive
3. click on download icon

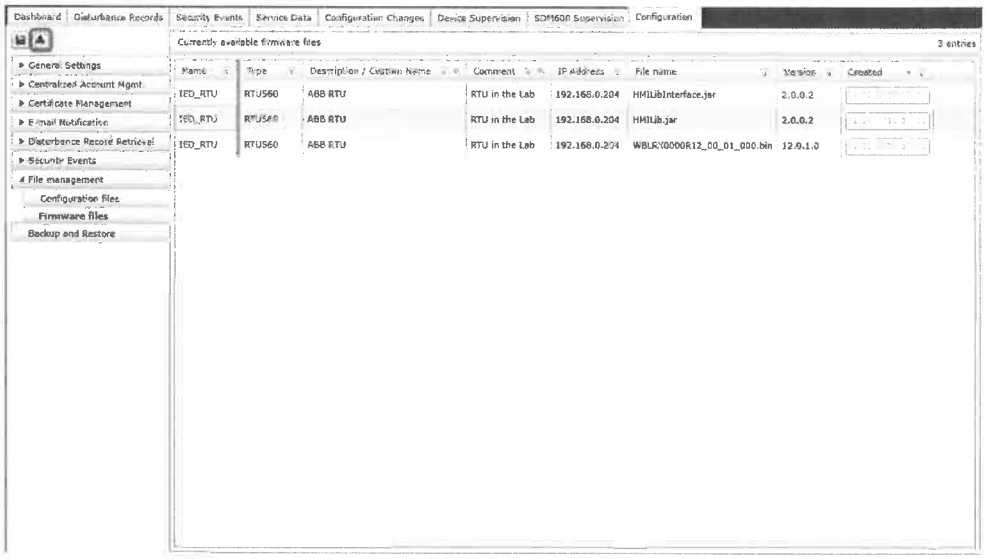


Figure 12.4: File management - read file from the drive

For the RTU specific configuration support follow this link:
http://new.abb.com/substation-automation/products/remote-terminal-units

13 Backup and Restore

Backup

SDM600 provides a function to back up the database and configuration. To take a backup, navigate to **Configuration Tab > Backup and Restore** subtab. Click **Backup Now**. A backup is created under the directory where *SDM600Databases* is installed. By default, the location of the backup files is under *C:\SDM600Databases\MSSQL10_50.SDMSERVER\MSSQL\Backup*. The file name has the *.sdmbakx* ending. SDM600 provides a possibility to back up the SDM600 database to a directory defined by the user. To do this, fill in the field for folder for SDM600 Backup.

It is important that the defined backup folder is a folder on the SDM600 server and not the local server where you access SDM600 (unless you access SDM600 locally).

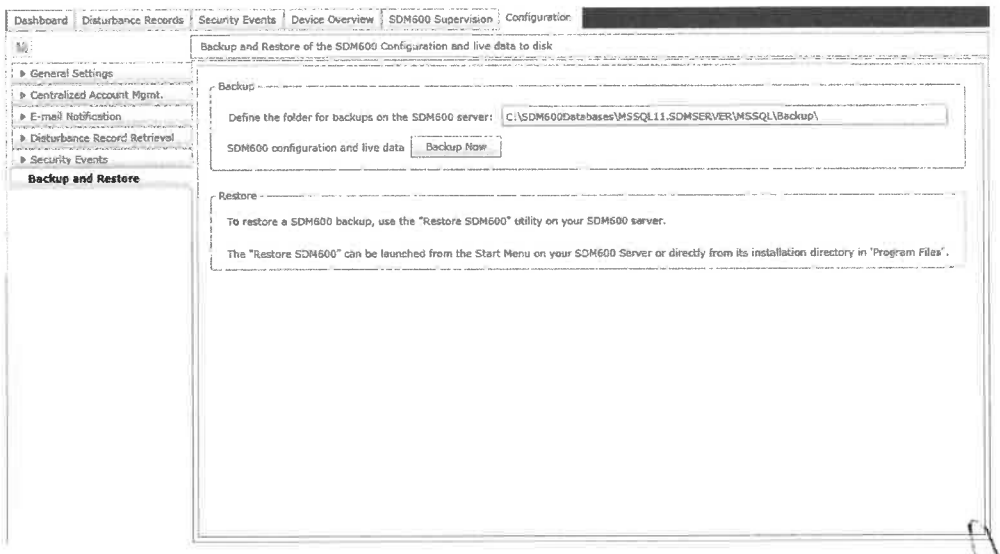


Figure 13.1: SDM600 Backup Functionality

It is also possible to create SDM600 backup, using *Restore SDM600* tool.

Navigate to Windows Start Menu on the SDM600 server and find SDM600 Restore Tool. Make sure that *Backup* tab is activated.

There is an option to backup configuration data only. If option is selected, then disturbance records data, configuration changes and security events data is not exported .

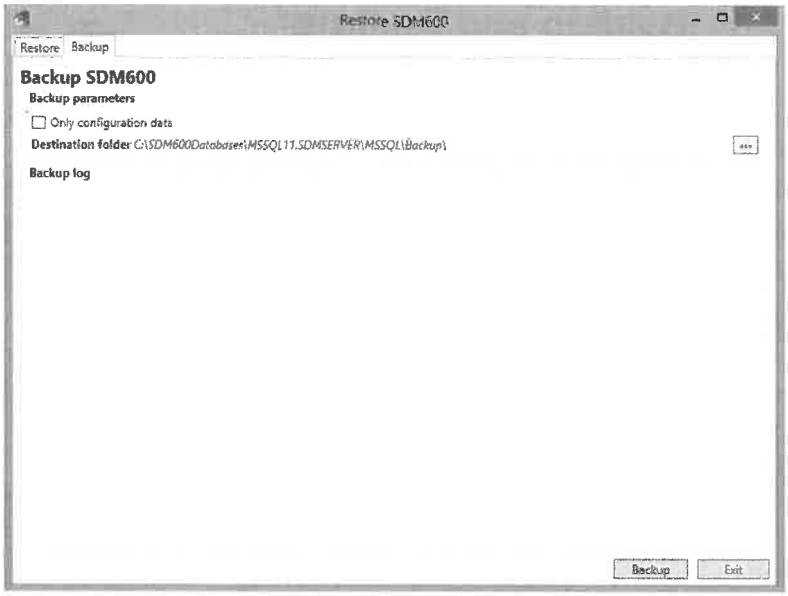


Figure 13.2: Backup tab in Restore SDM600 tool

Restore

SDM600 provides a function to restore all the data and configuration from the backup file. Restore operation will overwrite any existing data and any changes made since the last backup.

The SDM600 restore function is located in the folder where SDM600 is installed. By default, it is under *C:\Program Files (x86)\ABB\SDM600*.

To restore all the data and configuration from a backup file, do the following:

1. Navigate to the directory where SDM600 is installed (at the server side).
2. Navigate to Windows Start Menu on the SDM600 server and find SDM600 Restore Tool, or alternatively, Right-click the *RestoreSDM600Databases.bat* file, and from the context menu, select **Run as administrator**.

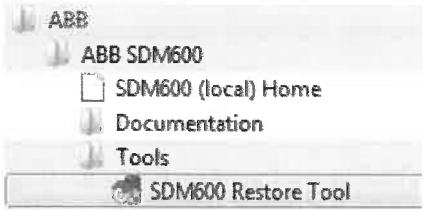


Figure 13.3: SDM600 Function to Restore the Backup - Access from Windows Start Menu

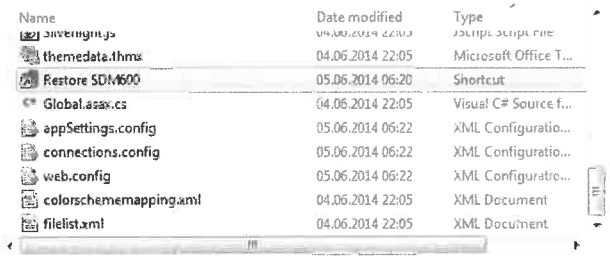


Figure 13.4: SDM600 Function to Restore the Backup

3. Make sure that *Restore* tab is active
4. After this, there are two options:

   - To create a backup of the current database before restoring a backup database.
   - To disable import of SDM600 live data. When this field is unchecked, only SDM600 configuration will be restored. Disturbance records data, configuration changes and security events data is not imported.

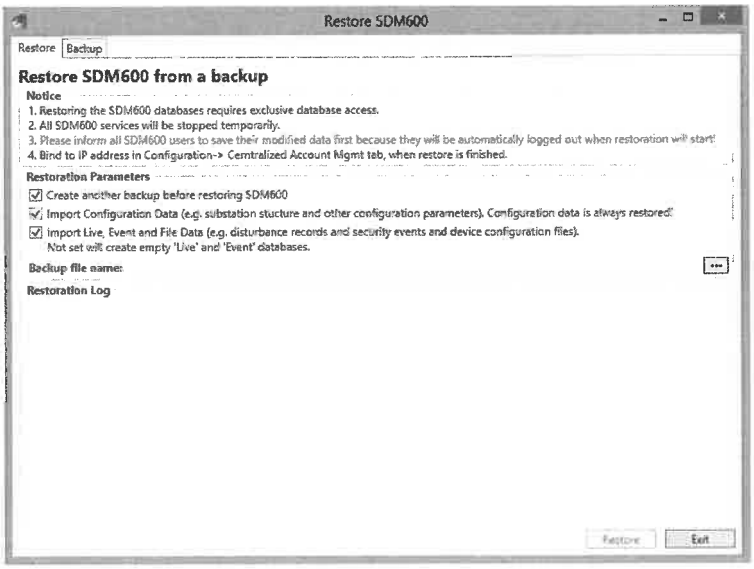


Figure 13.5: SDM600 Restore Function - Step 1 - Select Whether to Backup Current Data or Not

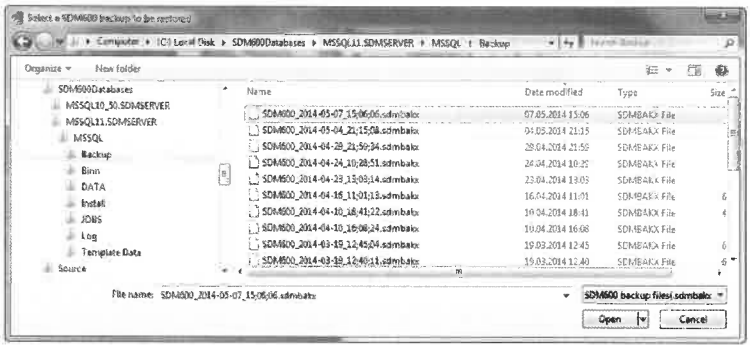


Figure 13.6: SDM600 Restore Function - Step 2 - Select Backup File

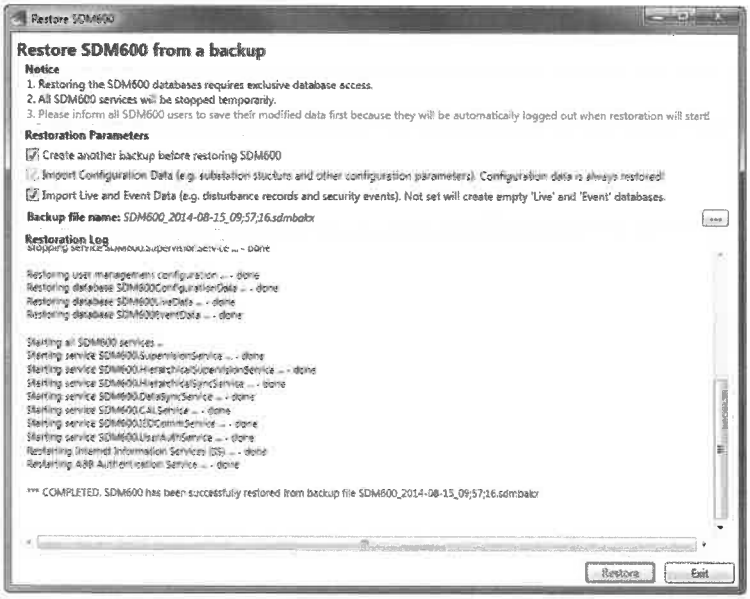


Figure 13.7: SDM600 Restore Function - Step 3 - Restore Process Complete

The SDM600 restore functionality requires that all the services are stopped before the restoration can be done. After the restoration is completed, all the services are automatically started. Therefore, it is important to make sure that during the restoration period no user is connected to SDM600.

Here are possible anomaly events when restoring the SDM600 backup:

- The SDM600 restore functionality requires that all the services are stopped before the restoration can be done. If the services cannot be stopped, the restoration process will be cancelled. If this happens, try again or restart the PC where SDM600 is installed.
- After restoring a backup, the SDM600 restore functionality restarts the services. If any of the services does not start properly, try to restart the computer. To check whether all services have been started, go to **Task Manager**, open the **Services** tab, and click **Services**. In a fully operational condition, all SDM600 services should be in the Started state. If a service is not up and running, the cause for this can be checked by navigating to **Windows Event Viewer > Windows Log > Application**. If this happens, please contact your SDM600 Supportline.

Restoring backup in an SDM600 parent child relationship has to be done with extra care, particularly on SDM600 Centralized Account Management feature. SDM600 Centralized Account Management requires the centralized account management database at the parent to always be in the most updated state than the one in the SDM600 children. In the case where a backup file that contains older centralized account management database needs to be restored at the SDM600 parent, there is a chance that centralized account management at SDM600 children will not receive any update from SDM600 parent. This is because the centralized account management at the SDM600 child has a newer data than the one in the centralized account management at the SDM600 parent. To overcome this situation, it is important to first stop the ABB Authentication Service. Next, delete the content of the SDM600 centralized account management Data folder from SDM600 children. By default, the Data folder can be found under C:\Program Files (x86)\ABB\SDM600\OpenLDAP\data. Next, restart the ABB Authentication Service, or simply conduct a full restart of the computer where SDM600 children is installed.

SDM600 Database Cleanup utility

The SDM600 provides possibility to clean up databases without uninstalling whole application.

There are two databases, which can be cleaned up:

- SDM600 configuration and live data database (stored in MS SQL)
- Users database (stored in Centralized Accounts Management DB)

In order to cleanup SDM600 database follow steps below:

1. Log in, as administrator, on the server, where SDM600 is installed.
2. Run command line tool with administrator privileges (click **Start**, in the search box type **cmd** and then press *CTRL+SHIFT+ENTER*)
3. Navigate to path where SDM600RestoreTool.exe is saved. (cd C:\Program Files (x86)\ABB\SDM600\bin).
4. a. Execute *SDM600RestoreTool.exe /CleanSDM600* command in order to delete SDM600 configuration and live data database or
   b. Execute *SDM600RestoreTool.exe /CleanUsers* command in order to delete users database or
   c. You can combine both parameters in order to delete all SDM600 databases. (*SDM600RestoreTool.exe /CleanSDM600 /CleanUsers*)

Notice that after cleaning up users database, SDM600 will ask for new administrator credentials and will create initial account (as is performed during first installation).

Appendix A List of ABB SDM600 Security Event EventIDs

Event ID	Type	Event Description	SDM600 Event Category
1110	Event	Login successful	Security Accountability
1115	Event	Password expired, Login successful	Security Accountability
1120	Alarm	Login failed - Unknown user	Potential Security Violation
1130	Event	Login failed - Wrong credentials	Potential Security Violation
1140	Event	Login failed - Wrong password	Potential Security Violation
1150	Alarm	Login failed - Password expired	Security Accountability
1170	Alarm	Login failed 3 times	Potential Security Violation
1180	Alarm	Login failed too many user sessions	Potential Security Violation
1210	Event	Logout (user logged out)	Security Accountability
1220	Event	Logout due to user inactivity (timeout)	Security Accountability
1310	Event	Connection with configuration tool successful	System Engineering and Configuration
1320	Event	Downloaded/wrote configuration successfully	System Engineering and Configuration
1321	Event	Configuration download started	System Engineering and Configuration
1322	Event	Configuration stored in the device successfully	System Engineering and Configuration
1330	Event	Uploaded/read configuration successfully	System Engineering and Configuration
1331	Event	Configuration upload started	System Engineering and Configuration
1340	Event	Downloaded/wrote firmware successfully	System Maintenance
1350	Event	Uploaded/read firmware successfully	System Maintenance
1352	Alarm	Stored certificates in the device successfully	System Operation
1356	Event	Extracted/exported archive file from device successfully	System Operation

Event ID	Type	Event Description	SDM600 Event Category
1357	Event	Extracted/exported diagnosis file from device successfully	System Operation
1358	Event	Extracted/exported certificates from device successfully	System Operation
1360	Event	Viewed parameter value(s) successfully	System Operation
1370	Event	Viewed Security Event logs successfully	Security Operation
1375	Event	Viewed disturbance records successfully	System Operation
1380	Event	Parameter changed successfully	System Engineering and Configuration
1390	Event	Downloaded Security Event list successfully	Security Operation
1400	Event	Configuration deleted successfully	System Engineering and Configuration
1410	Alarm	Connection with configuration tool failed	System Engineering and Configuration
1420	Event	Download/writing configuration failed	System Engineering and Configuration
1422	Event	Device configuration update failed	System Engineering and Configuration
1430	Event	Upload/read configuration failed	System Engineering and Configuration
1440	Event	Download/writing firmware failed	System Maintenance
1450	Event	Upload/read firmware failed	System Maintenance
1452	Event	Storing/writing certificates in the device failed	System Operation
1456	Event	Extracting/exporting archive file from the device failed	System Operation
1457	Event	Extracting/exporting diagnosis file from the device failed	System Operation
1458	Event	Extracting/exporting certificates from the device failed	System Operation
1460	Alarm	Parameter change failed - no rights	System Engineering and Configuration
1470	Event	Parameter change failed - out of range	System Engineering and Configuration
1480	Event	Parameter change failed - wrong type	System Engineering and Configuration
1490	Event	Download of Security Event list failed	Security Operation
1500	Alarm	Deletion of configuration failed	System Engineering and Configuration
1510	Event	Software update initiated successfully	System Maintenance
1520	Event	Software updated successfully	System Maintenance

Event ID	Type	Event Description	SDM600 Event Category
1610	Alarm	Device software update failed	System Maintenance
1660	Event	View of parameter failed	System Operation
1670	Event	View of Security Event list failed	Security Operation
1675	Event	View disturbance records failed	System Operation
1710	Alarm	Device reset to factory default	System Engineering and Configuration
1720	Alarm	User accounts reset to factory default	Security Administration and Configuration
1730	Alarm	Admin password reset to factory default	Security Administration and Configuration
2110	Event	User account created successfully	Security Administration and Configuration
2112	Event	User account added to replication group successfully	Security Administration and Configuration
2113	Event	User account removed from replication group successfully	Security Administration and Configuration
2115	Event	User account enabled successfully	Security Administration and Configuration
2117	Event	User account disabled successfully	Security Administration and Configuration
2120	Event	User account deleted successfully	Security Administration and Configuration
2130	Event	User account creation failed	Security Administration and Configuration
2132	Event	Addition of user account to replication group failed	Security Administration and Configuration
2133	Event	Removal of user account from replication group failed	Security Administration and Configuration
2135	Event	User account enabling failed	Security Administration and Configuration
2137	Event	User account disabling failed	Security Administration and Configuration

Event ID	Type	Event Description	SDM600 Event Category
2140	Event	User account deletion failed	Security Administration and Configuration
2160	Event	New role assigned to user successfully	Security Administration and Configuration
2161	Event	Permission changed successfully	Security Administration and Configuration
2162	Event	Permission added successfully	Security Administration and Configuration
2170	Event	User role assignment removed successfully	Security Administration and Configuration
2172	Event	User permission removed successfully	Security Administration and Configuration
2180	Event	New role created successfully	Security Administration and Configuration
2190	Event	Role deleted successfully	Security Administration and Configuration
2210	Event	User password changed successfully	Security Administration and Configuration
2220	Event	Change of user password failed	Security Administration and Configuration
2225	Event	User data changed successfully (for example, username, etc.)	Security Administration and Configuration
2226	Event	Change of user data failed	Security Administration and Configuration
2230	Event	New user role assignment failed	Security Administration and Configuration
2231	Event	Permission change failed	Security Administration and Configuration
2232	Event	Addition of permission failed	Security Administration and Configuration

Event ID	Type	Event Description	SDM600 Event Category
2233	Event	User password change failed - too short	Security Administration and Configuration
2235	Event	User password change failed - policy check failed	Security Administration and Configuration
2240	Event	User session role changed successfully	Security Administration and Configuration
2245	Event	User session role change failed	Security Administration and Configuration
2270	Event	Role assignment removal failed	Security Administration and Configuration
2272	Event	User permission removed failed	Security Administration and Configuration
2280	Event	New role creation failed	Security Administration and Configuration
2290	Event	Role deletion failed	Security Administration and Configuration
2310	Event	Password file downloaded successful	Security Operation
2320	Event	Password file uploaded successful	Security Operation
2350	Event	Download of password file failed	Security Operation
2360	Event	Upload of password file failed	Security Operation
2510	Alarm	Password file on CF card corrupted	Security Operation
2520	Alarm	Password file corrupted	Security Operation
3110	Event	TCP communication with security log subscriber successful	Communication
3120	Event	TCP communication with security log publisher successful	Communication
3150	Event	TCP communication with security log server successful	Communication
3190	Event	Ethernet reconnection	Communication
3210	Alarm	TCP communication with security log subscriber failed	Communication
3220	Alarm	Log data hash check failed (Log data altered)	Communication
3230	Alarm	TCP communication with security log publisher failed	Communication
3250	Alarm	TCP communication with security log server failed - Event not sent	Communication
3290	Alarm	Ethernet connection failure	Communication

Event ID	Type	Event Description	SDM600 Event Category
3420	Alarm	Security log file deleted by user	Potential Security Violation
3430	Event	SEC_Security log file deleted by system	System Engineering and Configuration
3440	Alarm	Security logs edited by user	Potential Security Violation
3710	Event	CAM server communication successful	Security Operation
3810	Alarm	CAM server communication failed	Security Operation
4110	Event	SSL connection successful	Security Operation
4120	Alarm	SSL connection/certificate accepted	Security Operation
4210	Alarm	SSL connection failed - Certificate validation failed	Potential Security Violation
4220	Alarm	SSL connection failed - IKE failed	Potential Security Violation
4310	Event	VPN connection successful	Security Operation
4350	Alarm	VPN connection failed - Negotiation failed	Potential Security Violation
4360	Alarm	VPN connection failed - IKE failed	Potential Security Violation
5110	Event	Manual reset	System Operation
5120	Event	Reset trips	System Operation
5130	Event	Reset LEDs	System Operation
5140	Event	Protection system restarted	System Operation
5150	Alarm	Control system restarted	System Operation
5152	Alarm	Control system restarted	System Operation
5160	Event	Gateway/RTU restarted	System Operation
5270	Alarm	System startup	System Operation
5272	Alarm	System startup failed	System Operation
5280	Event	System shutting down	System Operation
6110	Event	Test Mode started	System Operation
6112	Event	Starting of Test Mode failed	System Operation
6120	Event	Test Mode ended	System Operation
6130	Event	Control operation performed successfully	System Operation
6132	Event	Failed to perform a control operation	System Operation
6140	Event	Signal forced - value changed	System Operation
6150	Event	Test Event - to test routing configuration	System Operation
6160	Event	General command performed successfully	System Operation
6162	Event	Failed to perform a general command	System Operation

Event ID	Type	Event Description	SDM600 Event Category
6170	Event	Simulation Mode started	System Operation
6172	Event	Starting of Simulation Mode failed	System Operation
6175	Event	Simulation Mode ended	System Operation
6180	Event	Blocked Mode started	System Operation
6182	Event	Blocked of Simulation Mode failed	System Operation
6185	Event	Blocked Mode ended	System Operation
6210	Event	System time set manually successfully	System Engineering and Configuration
6310	Event	System time set manually failed	System Engineering and Configuration
6497	Alarm	Antivirus general info event, see antivirus logs for details	Security Operation
6498	Alarm	Antivirus general warning event, see antivirus logs for details	Security Operation
6499	Alarm	Antivirus general error event, see antivirus logs for details	Security Operation
6510	Alarm	Debug mode started successfully	System Maintenance
6515	Alarm	Starting Debug Mode failed	System Maintenance
6520	Event	Debug Mode ended	System Maintenance
6550	Event	Protocol logging mode started	System Maintenance
6560	Event	Protocol logging mode ended	System Maintenance
6570	Event	Service started successfully	System Operation
6571	Event	Service enabled successfully	System Operation
6572	Alarm	Failed to start service	System Operation
6573	Alarm	Failed to enable service	System Operation
6575	Alarm	Service stopped successfully	System Operation
6577	Alarm	Stopping of service failed	System Operation
6578	Event	Task started successfully	System Operation
6579	Alarm	Failed to start task	System Operation
6580	Event	Data capturing started successfully	System Operation
6582	Event	Start of data capturing failed	System Operation
6585	Event	Data capturing stopped successfully	System Operation
6587	Event	Stopping of data capturing failed	System Operation
6590	Alarm	MCM configuration changed successfully	System Operation

Event ID	Type	Event Description	SDM600 Event Category
6592	Alarm	Change of MCM configuration failed	System Operation
6595	Alarm	MCM configuration reset successfully	System Operation
6597	Alarm	Resetting of MCM configuration failed	System Operation
7110	Event	Switching device open	System Operation
7120	Event	Switching device close	System Operation
7310	Alarm	Hardware change detected	System Engineering and Configuration
8010	Alarm	Recovery of previous configuration successful	System Engineering and Configuration
8020	Event	Date and time set successfully	System Engineering and Configuration
8030	Event	New certificate generated successfully	System Engineering and Configuration
8040	Event	Communication system startup successful	System Operation
8050	Event	System backup performed successfully	System Operation
8060	Event	System backup started successfully	System Operation
8070	Event	System restore performed successfully	System Operation
8080	Event	System restore started successfully	System Operation
8210	Alarm	Recovery of previous configuration failed	System Engineering and Configuration
8220	Event	Date and time setting failed	System Engineering and Configuration
8230	Event	New certificate generation failed	System Operation
8240	Event	Communication system startup failed	System Operation
8250	Event	System backup failed	System Operation
8260	Event	Failed to start system backup	System Operation
8270	Event	Failed to restore the system	System Operation
8280	Event	Failed to start system restore	System Operation
9010	Alarm	Flooding attack detected	Potential Security Violation
9020	Alarm	Malformed packets attack detected	Potential Security Violation
9030	Alarm	Intrusion detected or Application blocked	Potential Security Violation
9040	Alarm	Intrusion detected	Potential Security Violation
9050	Alarm	Intrusion detected or Application blocked	Potential Security Violation
9060	Alarm	IDS detected unknown traffic	Potential Security Violation

Event ID	Type	Event Description	SDM600 Event Category
9070	Alarm	IDS detected illegal traffic	Potential Security Violation
9080	Alarm	IDS detected missing traffic	Potential Security Violation
9110	Alarm	Firewall blocked incoming connection	Potential Security Violation
9120	Alarm	Firewall blocked outgoing connection	Potential Security Violation
9130	Alarm	Firewall stopped/disabled	Security Operation
9140	Alarm	Firewall started/enabled	Security Operation
9150	Alarm	Firewall settings/rules changed successfully	Security Administration and Configuration
9210	Alarm	IPS blocked incoming packet	Potential Security Violation
9220	Alarm	IPS blocked incoming packet	Potential Security Violation
9230	Alarm	IPS stopped/disabled	Security Operation
9240	Alarm	IPS started/enabled	Security Operation
9250	Alarm	IPS settings/rules changed successfully	Security Administration and Configuration
9510	Alarm	CSR approved and certificate issued successfully	Security Administration and Configuration
9520	Alarm	Certificate signing request failed	Security Administration and Configuration
9610	Alarm	Certificate validation succeeded	Security Administration and Configuration
9620	Alarm	Certificate validation failed - Certificate expired	Security Administration and Configuration
9630	Alarm	Certificate validation failed - Certificate revoked	Security Administration and Configuration
9640	Alarm	Certificate validation failed - Certificate signature check failed	Security Administration and Configuration
9990	Event	Unidentified Syslog event	Unknown
9991	Event	Unidentified IEC 61850 event	Unknown
9995	Alarm	UAL Syslog FIFO receiver overflow, message overwritten	Security Operation

Event ID	Type	Event Description	SDM600 Event Category
10010	Event	Device successfully entered maintenance menu due to a user action	System Maintenance
10012	Event	Device failed to enter maintenance menu due to a user action	System Maintenance
10020	Event	Device successfully forced into maintenance menu due to new state	System Maintenance
10022	Event	Device failed to force maintenance menu after a new state	System Maintenance
10030	Event	FTP server successfully activated from maintenance menu	System Maintenance
10032	Event	Activation of FTP server from maintenance menu failed	System Maintenance
10040	Event	Firmware update procedure aborted successfully	System Maintenance
10042	Event	Failed to abort firmware update procedure	System Maintenance
10050	Event	Recovery menu entered successfully	System Maintenance
10052	Event	Failed to enter Recovery menu	System Maintenance
10060	Event	Authentication disabled from Maintenance menu successfully	System Maintenance
10062	Event	Failed to disable authentication from Maintenance menu	System Maintenance
10070	Event	Change lock disabled successfully from Maintenance menu	System Maintenance
10072	Event	Failed to disable change lock from Maintenance menu	System Maintenance
10080	Event	IEC 61850 disabled successfully from Maintenance menu	System Maintenance
10082	Event	Failed to disable IEC 61850 from Maintenance menu	System Maintenance
13200	Event	Configuration transferred to the device successfully	System Engineering and Configuration
13210	Event	Configuration transfer to the device started	System Engineering and Configuration
13220	Event	Configuration changed successfully	System Engineering and Configuration
13250	Event	Entered configuration mode successfully	System Engineering and Configuration
13260	Event	Exited configuration mode successfully	System Engineering and Configuration

Event ID	Type	Event Description	SDM600 Event Category
13300	Event	Configuration files read/exported from the device successfully	System Engineering and Configuration
13310	Event	Configuration exporting from the device started successfully	System Engineering and Configuration
13400	Event	Firmware transferred to the device successfully	System Engineering and Configuration
13500	Event	Firmware files read/exported from the device successfully	System Engineering and Configuration
13520	Event	Certificates transferred to the device successfully	System Engineering and Configuration
13560	Event	Exported/read archive file from the device successfully	System Engineering and Configuration
13570	Event	Exported/read diagnosis file from the device successfully	System Engineering and Configuration
13580	Event	Exported/read certificates from device successfully	System Engineering and Configuration
13900	Alarm	Security logs read/exported from the device successfully	Security Administration and Configuration
13910	Alarm	Security logs report generated successfully	Security Administration and Configuration
14200	Event	Failed to transfer configuration to the device	System Engineering and Configuration
14210	Event	Failed to start transfer of configuration to the device	System Engineering and Configuration
14220	Event	Failed to change the configuration	System Engineering and Configuration
14250	Event	Failed to enter configuration mode	System Engineering and Configuration
14260	Event	Failed to exit configuration mode	System Engineering and Configuration
14300	Event	Failed to read configuration files from the device	System Engineering and Configuration
14310	Event	Failed to start export of configuration from the device	System Engineering and Configuration
14400	Event	Failed to transfer firmware to the device	System Engineering and Configuration
14500	Event	Failed to read firmware files from the device	System Engineering and Configuration
14520	Event	Failed to transfer certificates to the device	System Engineering and Configuration
14560	Event	Failed to read archive file from the device	System Engineering and Configuration

Event ID	Type	Event Description	SDM600 Event Category
14570	Event	Failed to read diagnosis file from the device	System Engineering and Configuration
14580	Event	Failed to read certificates from the device	System Engineering and Configuration
14900	Event	Failed to read security logs from the device	Security Administration and Configuration
14910	Alarm	Failed to generate security logs report	Security Administration and Configuration
23100	Event	Password file transferred and stored in the device successfully	Security Operation
23200	Event	Password file read/exported from the device successfully	Security Operation
23500	Event	Failed to transfer password file to the device	Security Operation
23600	Event	Failed to read password file from the device	Security Operation
15010	Event	Controller mode changed to configuration mode successfully	System Engineering and Configuration
15020	Event	Controller mode changed to execute mode successfully	System Engineering and Configuration
15110	Alarm	Controller mode change to configuration mode failed	System Engineering and Configuration
15120	Alarm	Controller mode change to execute mode failed	System Engineering and Configuration
15200	Event	Bus IF mounted successfully	System Engineering and Configuration
15210	Event	Bus IF unmounted successfully	System Engineering and Configuration
15220	Event	Global device configuration updated successfully	System Engineering and Configuration
15230	Event	Configuration data initialized successfully	System Engineering and Configuration
15240	Event	Complete configuration data reloaded successfully	System Engineering and Configuration
15250	Event	CCO converted module process variables removed successfully	System Engineering and Configuration
15260	Event	Function diagrams commissioned successfully	System Engineering and Configuration
15270	Event	CCO process variable parameterized successfully	System Engineering and Configuration
15280	Event	Single parameter parameterized successfully	System Engineering and Configuration

Event ID	Type	Event Description	SDM600 Event Category
15290	Event	Single parameter simulated successfully	System Engineering and Configuration
15300	Event	Bus IF mounting failed	System Engineering and Configuration
15310	Event	Bus IF unmounting failed	System Engineering and Configuration
15320	Alarm	Global device configuration update failed	System Engineering and Configuration
15330	Event	Configuration data initialization failed	System Engineering and Configuration
15340	Event	Complete configuration data reload failed	System Engineering and Configuration
15350	Event	CCO converted module process variables removal failed	System Engineering and Configuration
15360	Event	Function diagrams commissioning failed	System Engineering and Configuration
15370	Event	CCO process variable parametrization failed	System Engineering and Configuration
15380	Event	Single parameter parametrization failed	System Engineering and Configuration
15390	Event	Single parameter simulation failed	System Engineering and Configuration
15410	Event	Profibus master/slave configured successfully	System Engineering and Configuration
15420	Event	Profibus channel configured successfully	System Engineering and Configuration
15430	Event	Profibus parameterized channel configured successfully	System Engineering and Configuration
15440	Event	Profibus master/slave configuration reloaded successfully	System Engineering and Configuration
15450	Event	Profibus channel configuration reloaded successfully	System Engineering and Configuration
15510	Alarm	Profibus master/slave configuration failed	System Engineering and Configuration
15520	Alarm	Profibus channel configuration failed	System Engineering and Configuration
15530	Alarm	Profibus parameterized channel configuration failed	System Engineering and Configuration
15540	Event	Profibus master/slave configuration reload failed	System Engineering and Configuration
15550	Event	Profibus channel configuration reload failed	System Engineering and Configuration
15610	Event	IEC 61850 stack initialized successfully	System Operation

Event ID	Type	Event Description	SDM600 Event Category
15620	Event	IEC 61850 stack configured successfully	System Engineering and Configuration
15630	Event	IEC 61850 stack configuration reloaded successfully	System Engineering and Configuration
15710	Event	IEC 61850 stack initialization failed	System Operation
15720	Alarm	IEC 61850 stack configuration failed	System Engineering and Configuration
15730	Event	IEC 61850 stack configuration reload failed	System Engineering and Configuration
15810	Event	Control parameter read and view from device successfully	System Operation
15850	Event	Operable parameters read from device into project data base successfully	System Operation
15860	Event	Operable parameters transferred and stored into the device successfully	System Operation
15890	Event	Generic DTM event	System Operation
15910	Event	Failed to read control value parameter from device	System Operation
15950	Event	Failed to read operable parameters from device into project data base	System Operation
15960	Event	Failed to transfer and store operable parameters into the device	System Operation

Appendix B Mapping Windows Events to ABB SDM600 Security Event EventIDs

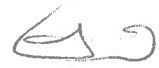
EventID	Successful Windows Event result	Fail Windows Event Result	Event Description
1102	3420		Security log file deleted by user
4608	5270	5272	System startup
4609	5280		System shutting down
4616	8020	8220	Date and time set
4624	1110		Login successful
4625		1130	Login failed
4634	1210		Logout (user logged out)
4647	1210		Logout (user logged out)
4649	9020		Flooding attack detected
4650, 4651	4310	4350	VPN connection
4652, 4653, 4654	4350	4350	VPN connection failed - Negotiation failed
4704	2162	2232	Permission added
4705	2172	2272	User permission removed
4720	2110	2130	User account created
4722	2115	2135	User account enabled
4723	2220	2220	Change of user password failed
4724	2220	2220	Change of user password failed
4725	2117	2137	User account disabled
4726	2120	2140	User account deleted
4774	1110	1130	Login
4775	1130	1130	Login failed - Wrong credentials
4887	9510	9520	CSR approved and certificate issued successfully
4888	9520	9520	Certificate signing request failed
4946, 4947, 4948, 4950	9150		Firewall settings/rules changed
4976, 4977, 4978	4350	4350	VPN connection failed - Negotiation failed

EventID	Successful Windows Event result	Fail Windows Event Result	Event Description
4979, 4980, 4981, 4982	4310	4350	VPN connection successful
4983, 4984	4350	4350	VPN connection failed - Negotiation failed
5031	9110		Firewall blocked incoming connection
5148	9010		Flooding attack detected
5152	9210	9210	IPS blocked incoming packet
5155	9110	9110	Firewall blocked incoming connection
5451	4310	4360	VPN connection successful
5453	4360	4360	VPN connection failed - IKE failed

Appendix C Self-Generated SDM600 Security Events

EventID	Event Description	Cause of Event in SDM600
1110	Login successful	When a user successfully logged into SDM600
1115	Password expired, login successful	When a user manages to log in even if the user's password has expired
1130	Login failed - Wrong credentials	When a user enters a wrong combination of username and password
1210	Logout (user logged out)	When a user logged out from SDM600
2110	User account created successfully	When a new user account is successfully created
2120	User account deleted successfully	When a user account is successfully deleted
2160	New role assigned to user successfully	When a new role is successfully assigned to a user
2161	Permission changed successfully	When a user adjusts the SDM600 role to right mapping
2170	User role assignment removed successfully	When a user role is successfully removed from a user's role assignment
2210	User password changed successfully	When a user changes their password by entering correct required credentials
2220	Change of user password failed	When a user changes their password by entering a wrong combination of the required credentials
2225	User data changed successfully (for example, username, etc.)	When a user changes their data
8030	New certificate generated successfully	When a user requests SDM600 to generate a certificate and the certificate is successfully generated
8050	System backup performed successfully	When a user requests SDM600 to perform a system backup and the request is executed successfully
8230	New certificate generation failed	When a user requests SDM600 to generate a certificate and the certificate is not successfully generated

EventID	Event Description	Cause of Event in SDM600
8250	System backup failed	When a user requests SDM600 to perform a system backup and the request is not executed successfully
13200	Configuration transferred to the device successfully	When a user requests SDM600 to generate configuration files for another application or device to integrate it into ABB SDM600 Centralized Account Management and Centralized Activity Logging and the configuration files successfully generated and saved to user preferred location
13220	Configuration changed successfully	When a user conducts any configuration changes in SDM600 and the configuration is successfully applied
13520	Certificates transferred to the device successfully	When a user manages to export the credential that is used to sign certificates for all devices
14200	Failed to transfer configuration to the device	When a user requests SDM600 to generate configuration files for another application or device to integrate it into ABB SDM600 Centralized Account Management and Centralized Activity Logging and the configuration file fails to generate or configuration files are not saved properly to user preferred location
14220	Failed to change the configuration	When a user conducts any configuration changes in SDM600 and the configuration is not successfully applied
14520	Failed to transfer certificates to the device	When a user fails to export the credential that is used to sign certificates for all devices



Contact us

ABB Oy
Grid Automation Products
P.O. Box 614
FI-65101 Vaasa
Finland
Tel. +358 10 22 11
Fax. +358 10 224 1094

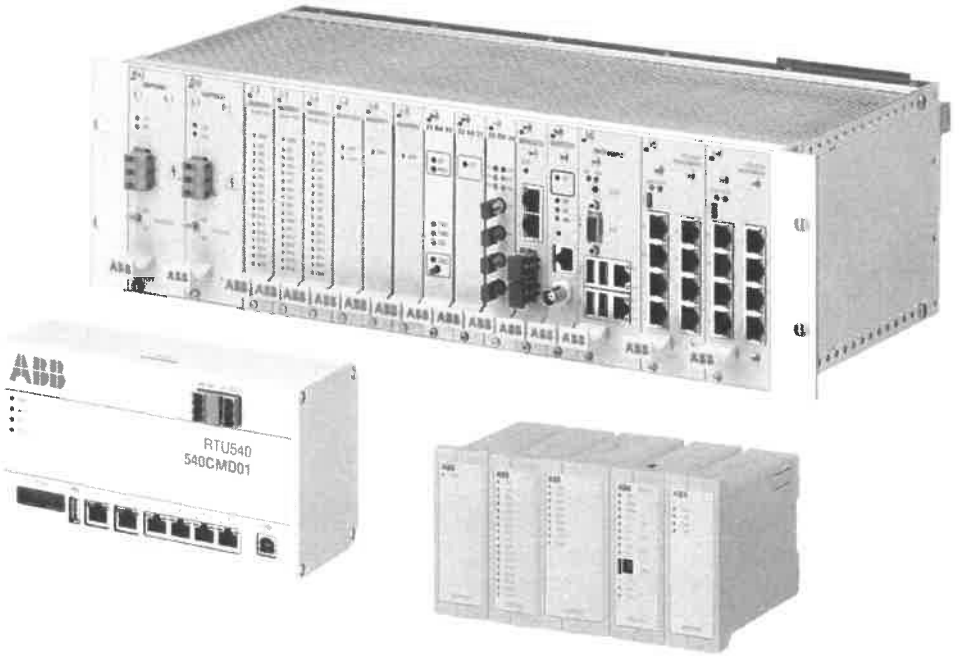
www.abb.com/substationautomation

Power and productivity
for a better world™

Power Grids

Remote Terminal Units Security Deployment Guideline

User manual



Revision

Document identity:		1KGT 150 925 V005 1
Revision	**Date**	**Description**
0	06/2016	Initial version for Release 12
1	11/2016	New chapter "Patch management" has been added (PR#32927)
2	06/2017	Chapter 'Virtual Private Network' has been updated (PR#2092)
3	09/2017	Updated table "IEEE 1686 compliance" (#35786)
	10/2017	Updated table 'Security event types' (PR#33956)
4	04/2018	Added chapter 'Intended Use' (PR#36874)
5	10/2018	Updated 'Permission Definition' table (PR#38263)
		Added feature Central User Account Management (CAM) (PR#2594)

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

Contents

1 Secure access

1.1 Secure system setup

As a communication gateway the RTU500 series connects a control system with a directly connected process or with subordinated devices. The connection to the control system can be serial point to point or Ethernet network based.

- The Ethernet communication protocols supported by the RTU500 series (e.g. IEC60870-5-104, DNP3) don't provide authentication or encryption of the communication.
- The RTU500 series Web server access is protected by authentication and with secure HTTPS communication. In the default setup the Web server communication is HTTPS.
- The access from the Integrated HMI is protected by authentication but the communication is done with a not encrypted proprietary protocol.

These security drawbacks are acceptable in limited local networks. For wide area networks in particular with connection to the Internet, additional configurations are required to increase protection and privacy for the RTU500 series Ethernet communication. This requirement could be fulfilled by a secure Virtual Private Network (VPN) configured with external devices or RTU500 series internal functionality.

The goal of network security is to provide confidentiality, integrity and authenticity:

- Confidentiality (keeping the data secret from the unintended listeners on the network)
- Integrity (ensuring that the received data is the data was actually sent)
- Authenticity (providing the identity of the endpoint to ensure that the end point is the intended entity to communicate with)

1.1.1 Virtual Private Network with external devices

The figure below shows a possible system setup in schematic form.

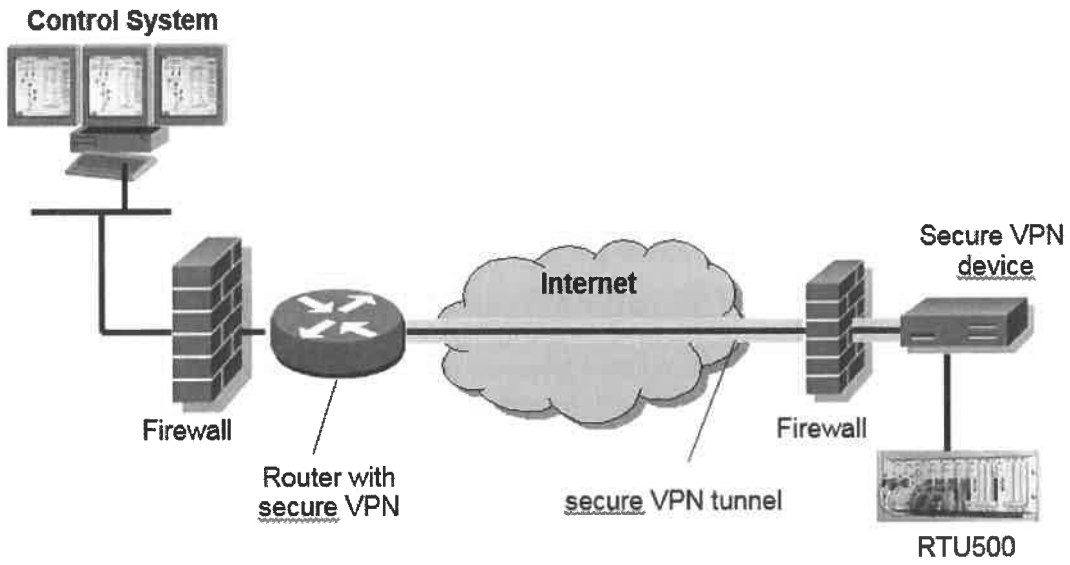


Figure 1: RTU500 series secure system setup with external VPN device

In this system setup the achieved protection and privacy is accomplished by

- A secure VPN uses cryptographic tunneling protocols to provide the intended confidentiality (blocking intercept and thus packet sniffing), sender authentication (blocking identity spoofing), and message integrity (blocking message alteration).
- A firewall to block unauthorized access while permitting authorized communications.

The security guide line cannot suggest concrete products for a secure system setup. This must be decided along the specific project, requirements and existing infrastructure. The required external equipment can separated devices or devices that combines firewall, router and secure VPN functionality.

1.1.2 Virtual Private Network with RTU500 internal functionality

The RTU500 series Virtual Private Network protocol implementation provides a standard method for transporting IP datagrams over a secured communication channel. The used technique for creating VPNs in RTU500 series is IPsec.

With the help of VPN a RTU can be connected to control system via the public internet. The data exchange is secured via the VPN connection. From the user point of view it looks like the RTU500 series resides within the NCC network.

The following picture shows a typical configuration:

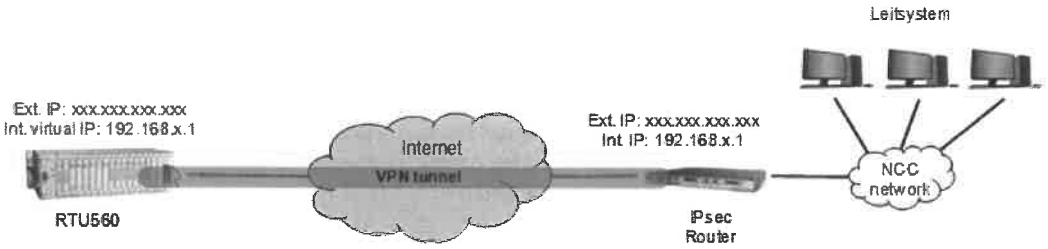


Figure 2: RTU500 series secure system setup with internal VPN interface

The RTU establishes a VPN connection to the IPsec Router. The VPN tunnel (red line) connects the virtual RTU network with the NCC network. Therefore a network-to-network connection is established. This connection is transparent and secured.

If a connection is established, the RTU can be accessed by a control system using the internal virtual IP address. All IP based protocols can run on this connection.

The RTU500 series supports two authentication methods:

- Pre-Shared Key (maximum length is 64 characters)
- X.509 Certificates

The RTU500 series supports the following features:

- Perfect Forward Secrecy: IKE performs a new DH exchange when rekeying the IPsec SAs
- Dead Peer Detection (DPD): a traffic-based method of detecting dead peers
- UDP Encapsulation and NAT-Traversal: enabling IPsec packets to traverse NAT devices

The RTU internal firewall discards all packets which are not related with the VPN tunnel except HTTPS when enabled.

For more detailed information about VPN functionality in RTU500 series, see RTU500 series function description - part 9: Interfaces and networks (1KGT 150 896).

1.2 Ethernet ports

To setup an Ethernet firewall the following table summarizes the Ethernet ports used in the RTU500 series. The ports are listed in ascending order. The column "Default state" defines whether a port is open or closed by default. All ports that are closed by default are opened by configuration or by online enabling.

Port	Protocol	Default state	Service	Comment
80	TCP	open	HTTP	Web server
102	TCP	closed	IEC 61850	Communication protocol
123	UDP	closed	SNTP	Time synchronization
161	UDP	closed	SNMP	Supervision client
389	TCP	closed	LDAP	CAM client
443	TCP	open	HTTPS	Web server
500	UDP	closed	IKE	ISAKMP packets
502[1]	TCP	closed	Modbus TCP	Communication protocol
514	UDP	closed	Syslog	External security log server
1793	TCP	closed	RIO server	Server for protocol logging
2000	UDP	closed	DNP3	Communication protocol
2404	TCP	closed	IEC60870-5-104	Communication protocol
4500	UDP	closed	IKE	ISAKMP NAT-T packets
5007	UDP	closed	IEC 61850	Debug trace port
5014	TCP	closed	Syslog/ArcSight	External security log server
17185	UDP	closed	VxWorks	Tornado debug port
19998[1]	TCP	closed	IEC60870-5-104	Secured communication
20000[1]	TCP	closed	DNP 3	Communication protocol
20547	TCP	closed	ProConOS	PLC program
50001	TCP	closed	HMI	Local HMI

Table 1: Ethernet ports used in RTU500 series

1 Configurable

The detail information about each port could be found in the next chapters. The ports are grouped according the purpose.

In case the CMU of an RTU500 provides more than one Ethernet interface, a network functionality can be assigned to a single interface or to several interfaces. In both applications the Ethernet ports of the network functionality are opened on the assigned interfaces only. On the other interfaces the ports are still closed. This behavior is achieved by the internal firewall of the RTU500 series.

1.2.1 Communication protocols

The RTU500 series supports several Ethernet communication protocols. These protocols are IEC 61850, Modbus TCP, IEC60870-5-104 and DNP3. All these communication protocols are enabled by configuration. That means the Ethernet port of a protocol is closed and not available if the configuration of the RTU doesn't contain a communication line of the protocol. If a protocol is configured the corresponding Ethernet port is open all the time.

Please refer to the RTUtil500 Users Guide and the corresponding protocol documentation on how to configure a certain communication protocol for the RTU500 series.

There are some restrictions and dependencies:

- The Ethernet ports used for Modbus TCP, DNP3 and secured IEC60870-5-104 communication line are configurable (in RTUtil500). The values in the table above are the default values defined in the protocol standard.
- The Ethernet ports used for IEC 61850 and IEC60870-5-104 are fixed and could not be changed.
- The communication protocol DNP3 could operate on UDP (default port 2000) or TCP (default port 20000). It is defined in the configuration which type of Ethernet protocol is used. Only one type is possible for a specific configuration.
- The debug trace port for IEC 61850 (port 5007) is not required for the normal protocol communication. That means a firewall can block this port without backlash to the protocol communication. The trace port is used for commissioning and error detection. The IEC 61850 debug trace port is closed by default and must be opened for logging within the RTU500 web server.

1.2.2 Central user account management

Besides the local user account management (LAM) the RTU500 series supports a central user account management (CAM). In this setup the RTU500 series acts as client to an external CAM server that manage all user accounts within a system.

The CAM client can be configured as functionality in the RTU. The functionality is assigned to one or more CMU Ethernet interfaces in a RTU. Only if the CAM client is configured on a CMU module the Ethernet port of the LDAP service is open on that CMU interface. On all other CMU interfaces the port is closed. If a CAM client is configured the corresponding port is open all the time. The default port for the LDAP service is 389.

Please refer to chapter "Central user account management" for detailed information about the functionality and the configuration of the central user account management.

1.2.3 Web server

The Web server is enabled by default on each Ethernet capable CMU of an RTU. In a multiple CMU system the Web server can be disabled by configuration on selected CMU's. In this case the HTTP and HTTPS Ethernet ports are closed. At least on one CMU the Web server must be enabled to be able to access the RTU. This requirement is enforced by the configuration tool RTUtil500.

To provide encryption and secure identification in the communication to the Web server the RTU500 series supports Hypertext Transfer Protocol Secure (HTTPS). This option is enabled by default. See chapter "Secure Web server access" for more information.

The Web server uses only HTTPS port and optional the HTTP and HTTPS port can be activated. No other ports are required by the RTU500 series Web server.

The Web server requires the following technical features that must be supported and enabled by the used Web client:

- HTTP 1.1
- HTML5
- CSS3
- JavaScript 1.8
- WebSocket

- HTTP Digest Access Authentication
- HTTP session cookies

In case of HTTPS access the Web client must support:

- HTTPS via TLS 1.2

Recommended as Web clients are:

- Google Chrome 70.0 or higher
- Microsoft Internet Explorer 11.0 or higher
- Mozilla Firefox 63.0 or higher
- Opera 53.0 or higher

The access to the RTU500 series Web server is protected by an authentication request for user name and password. In case the local user account management is used for authentication, HTTP Digest Access Authentication (DAA) protects the Web server access. DAA ensures that the user credentials are encrypted secure before sending over the network. Detailed information about DAA could be found in RFC2617 "HTTP Authentication: Basic and Digest Access Authentication".

If a central user account management server is configured the access to the Web server is protected by a HTTP form-based login dialog. In this case user credentials are not encrypted before sending over the network. For this setup secure Web server access via HTTPS is highly recommended to secure the transmission of the user credentials.

The administration of local user accounts is done in the RTU500 series Web server. See chapter "Local user account management" for more information.

If the Microsoft Internet Explorer is used as Web client the advanced option "Show friendly HTTP error messages" shall be disabled. Without this option the detailed error information of the RTU500 series Web server are shown. The option can be found in the "Advanced" tab of the "Internet Options".

1.2.4 Integrated HMI

The Integrated HMI can be configured as functionality in the RTU. The functionality is assigned to one or more CMU Ethernet interfaces in a RTU. Only if the Integrated HMI is configured on a CMU module the Ethernet port of the HMI is open on that CMU interface. On all other CMU interfaces the port is closed. If an Integrated HMI is configured the corresponding port is open all the time.

Please refer to the RTUtil500 Users Guide and the Integrated HMI documentation on how to configure the Integrated HMI for the RTU500 series.

1.2.5 User logging/debug interface

The RTU provides functionality to support the user in installation and commissioning. These are a functionality to monitor communication protocols (RIO protocol logging) and a programmable logic controller (PLC) for user written programs. Both functionalities use an Ethernet connection with the defined services (see table above). The following rules apply for the connections:

- The access to both functionalities is disabled by default and the corresponding Ethernet ports are closed.
- The access could be enabled in the RTU Web server. In this case the Ethernet port became open and an online connection could be established. The access is enabled for a specific CMU only.

- The access is disabled again if the online connection is closed or a fix timeout of 30 minutes is expired. By disabling the Ethernet port became closed.
- The administrator can prohibit the access to both functionalities. That means it is not possible to enable the functionality. See chapter "User interface" for information how to prohibit the access.
- The RIO protocol logging is available on every CMU independent from the configuration.
- The PLC debug interface is available only if a PLC is configured on a CMU. If not access is not possible and the corresponding Ethernet port is closed.

Please refer to the RTU500 series Web server documentation on how to enable the access to the RIO protocol logging and the PLC debug interface.

1.2.6 Time synchronization

The RTU500 series supports SNTP time synchronization as client and server. By configuration the functionality is assigned to one or more CMU Ethernet interfaces in an RTU. Only if an SNTP client or server is configured on a CMU module, the Ethernet port of SNTP is open on that CMU interface. On all other CMU interfaces the port is closed. If an SNTP client or server is configured the corresponding port is open all the time.

Please refer to the RTU Function Description for detailed information about the SNTP time synchronization.

1.2.7 Network management

For supervision of network devices the RTU500 series support SNMP as client. By configuration the functionality is assigned to one or more CMU Ethernet interfaces in an RTU. Only if an SNMP client is configured on a CMU module, the Ethernet port of SNMP is open on that CMU interface. On all other CMU interfaces the port is closed. If an SNMP client is configured the corresponding port is open all the time.

Please refer to the RTU500 series Function Description for detailed information about the SNMP client functionality.

1.2.8 External security log Server

Security relevant user operations within the RTU are logged as security events. These security events can be sent to external security log servers. The RTU500 series supports the following protocols/ports for external log servers:

- Syslog UDP via configurable port (default port = 514)
- Syslog TCP via configurable port (default port = 5014)
- ArcSight TCP via configurable port (default port = 5014)

By configuration the support of external log servers is assigned to one or more CMU Ethernet interfaces in an RTU. Only if an external log server is configured on a CMU board, the Ethernet port of the protocol is open on that CMU interface. On all other CMU interfaces the ports are closed. If an external log server is configured, the corresponding port is open all the time.

Please refer to chapter “Security event logging” for detailed information about external security log servers.

1.2.9 Developer debug interface

For maintenance purposes the RTU supports two developer debug interfaces. The first is an interface to the RTU firmware via the operating system VxWorks. The second interface is for monitoring the IEC 61850 communication (IEC 61850 debug trace interface). These interfaces allow direct access to the RTU on firmware level. The interfaces permit monitoring and manipulation. Therefore the interfaces must be handled with extremely caution.

The following rules apply for the developer debug interfaces:

- The debug interfaces are not required for the RTU functionality. Therefore a firewall must block the corresponding Ethernet ports.
- The access to the debug interfaces is disabled by default and the corresponding Ethernet ports are closed.
- The access could be enabled in the RTU500 series Web server. In this case the Ethernet port became open and an online connection could be established. The access is enabled for a specific CMU only. For enabling the debug interfaces administrator permissions are required.
- Once enabled, the debug interfaces must be disabled explicit in the RTU500 series Web server. This closes the Ethernet ports. For disabling the debug interfaces administrator permissions are required.

For more detailed information about protocol logging in RTU500 series, see RTU500 series function description - part 9: Interfaces and networks (1KGT 150 948)

1.2.10 Virtual Private Network

For a secure system setup over the public internet the RTU500 series supports the Virtual Private Network protocol IPsec. The VPN functionality could be configured once per CMU (on Ethernet interface E1 or E2 or PPP interface). Only if the VPN functionality is configured for a CMU interface the IPsec/IKE Ethernet ports are open on that interface. On all other CMU interfaces the ports are closed. If configured the corresponding IPsec/IKE ports are open all the time.

For more detailed information about VPN functionality in RTU500 series, see RTU500 series function description - part 9: Interfaces and networks (1KGT 150 948)

1.3 Encryption Algorithm

In the RTU encryption and hash algorithms are used to protect the access to the Web server, for the VPN communication and to encode the password file.

The algorithms are:

- AES (Advanced Encryption Standard), a block cipher based on a symmetric key algorithm to encrypt and decrypt information. The effective key length of the used AES-128 is 128 bits.
- SHA (Secure Hash Algorithm) a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST). In the RTU500 series the SHA-2 variants SHA-256, SHA-384 and SHA-512 are used.
- RSA (Rivest, Shamir and Adleman), an algorithm for public-key cryptography using a mathematically related key pair: a secret private key and a published public key. In the RTU RSA with an effective key length of 2048 bits is used.
- Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

- Blowfish is a symmetric-key block cipher algorithm, designed in 1993. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits.
- DES (Data Encryption Standard), a block cipher based on a symmetric key algorithm to encrypt and decrypt information. The effective key length of DES is 56 bits.
- Diffie–Hellman key exchange (DH), a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. In the RTU Diffie-Hellman with an effective key length of 2048 bits is used.
- Message-Digest algorithm 5 (MD5), a cryptographic hash function with a 128 bit hash value (see RFC1321 "The MD5 Message-Digest Algorithm" for detailed information). Used in the RTU500 series for HTTP Digest Access Authentication with quality of protection (protection of Web server access).
- Salsa20, a stream cipher submitted to the eSTREAM project by Daniel Bernstein (see "The Salsa20 family of stream ciphers" by Daniel J. Bernstein). In the RTU the reduced-round cipher Salsa20/12 with an effective key length of 56 bits is used. This cipher is included for migration from older RTU500 firmware version only. In the actual RTU500 firmware version the cipher is not used for encrypting and decrypting.

In the RTU500 series VPN implementation for IKE the following cryptographic encryption algorithms are supported:

- 3DES
- AES 128 CBC
- AES 192 CBC
- AES 256 CBC
- Blowfish
- DES

RTU500 series IKE implementation supports the following Diffie-Hellmann groups:

- MODP group 1 (768-bit)
- MODP group 2 (1024-bit)
- MODP group 5 (1536-bit)
- MODP group 14 (2048-bit)
- MODP group 15 (3072-bit)
- MODP group 16 (4096-bit)
- MODP group 17 (6144-bit)
- MODP group 18 (8192-bit)

1.4 Intended Use

Details concerning intended use:

- The intended use of the RTU500 is to use it in isolated networks
- It is not intended to connect the RTU500 or the RTU Web server direct to the internet
- In case the RTU500 is using public networks the VPN functionality inside the RTU500 is available

2 Local user account management

The local user account management in the RTU500 series outlines the functionality to administrate the persons that access the RTU. The key features provided by the local user account management are:

- User authentication based on user names and passwords
- User authorization based on roles and permissions
- Support of password policies
- Secure transmission of passwords from Web server and integrated HMI
- Secure storing of passwords on file system
- Download/Upload user account configurations

The following chapters describe first the design principles and later on the concrete user interface of the local account management. The description of the optional central user account management can be found in chapter "Central user account management".

2.1 Design principles

2.1.1 Account information

In the RTU500 series there are user accounts, account permissions and user roles. These terms have the following meaning:

- The user account represents a person that should access the RTU. The person is identified by a user name and a password.
- Account permissions are actions that a user could perform and requires authorization.
- User roles are groups of account permissions that could be assigned to users.

The relationship between user, role and permission is shown in the figure below.

Figure 3: Relationship user, role and permission

A user role can contain several permissions and a user account can be assigned to several user roles.

The account information are stored in a password file. The password file contains the list of defined users and their password, the list of user roles, the list of permissions and the assignment of user, permissions and roles. The permissions available within the RTU500 series are predefined and cannot be changed (see next chapter "Account Permissions"). The users, roles and assignments can be changed according the needs.

2.1.2 Account permissions

The account permissions available in the RTU500 series are fix defined and cannot be changed. Each defined account permission allows several actions within the RTU500 series Web server or Integrated HMI. The table below shows all available permissions and describes the allowed actions for every permission in detail.

Permission Definition	Description
viewData@ABBRTU500	Read and view RTU data: • View system diagnostics log in Web server. • View and download system diagnostics file in Web server. • View RTU500 series process data in hardware tree of Web server. • Enable and disable RIO protocol logging mode in the Web server. Once enabled there is no restriction on the access to the RIO server. That means the real access is not protected by user name and password. The RIO protocol logging mode is disabled after a fix timeout of 30 minutes if no online connection exists. • View and download process archive information via the Web server (events and indications, measured values and integrated total). • Download archived disturbance record files via the Web server. • View online parameter changes in the engineering part of the Web server. • View online configuration in the engineering part of the Web server.
config@ABBRTU500	Change configuration files: • Upload and download all RTU500 series configuration files via the Web server. This comprises the RTU configuration and the Integrated HMI configuration. • Restart of RTU500 series via RTU500 series Web server.
firmware@ABBRTU500	Change firmware files: • Upload and download all RTU500 series firmware files via the Web server. This comprises the RTU basic firmware, the communication controller firmware and the Integrated HMI firmware. • Restart of RTU500 series via RTU500 series Web server. • View, upgrade and extend RTU500 series protocol/function licenses (via Web server).
usrAccount@ABBRTU500	User account management: • Add, modify and delete user accounts (via Web server). • Add, modify and delete user roles (via Web server). • Assign and withdraw user accounts to user roles (via Web server). • Assign and withdraw account permissions to user roles (via Web server). • Change user passwords (via Web server). • Upload and download password files (via Web server). • Prohibit RIO protocol logging mode (via Web server). • Prohibit PLC online debug mode (via Web server). • Prohibit RTU500 series test mode (via Web server). • Prohibit online configuration changes (via Web server). • Prohibit online parameter changes (via Web server).
usrRole@ABBRTU500	User role management: • Assign and withdraw user accounts to user roles (via Web server).

Table 2: Account permissions available in the RTU

Permission Definition	Description
	• Assign and withdraw account permissions to user roles (via Web server). • Change user passwords (via Web server).
viewSecEvent@ABBRTU500	View security event logging / audit trails: • View logged security events in Web server. • Download logged security events in predefined CSV format (via Web server).
enableTest@ABBRTU500	Enabling and use simulation and test mode: • Enable/Disable RTU500 series test mode via the Web server. The test mode allows the simulation of inputs/ outputs in the test manager of the Web server. • Enable/Disable time administration test mode to allow setting of the RTU system time via the Web server. • Enable/Disable IEC 61850 startup logging (via Web server). • Enable/Disable Ethernet and PPP interface logging (via Web server). • Enable/Disable IEC 61850 debug trace interface (via Web server). • Enable/Disable VxWorks debug interface (via Web server). • Simulate inputs, outputs, system events and security events in the RTU500 series test mode via the Web server (If test mode is enabled). • Set system time of RTU via Web server, if time administration test mode is enabled.
enablePlc@ABBRTU500	Enable and use PLC online debug mode: • Enable/Disable PLC online debug mode via the Web server. Once enabled there is no restriction on the access to the PLC. That means the real access is not protected by user name and password. The PLC debug mode is disabled after a fix timeout of 30 minutes if no online connection exists.
onlineConf@ABBRTU500	Online configuration changes: • Online configuration changes (Engineering via the RTU500 web server)
onlinePara@ABBRTU500	Online parameter changes: • Online parameter changes (Engineering via the RTU500 web server)
viewDataHmi@ABBRTU500	Read and view data on the Integrated HMI: • View all configured Integrated HMI pages. • View and download process archive information in the HMI event list (events and indications, measured values and integrated total). • Acknowledge alarms in the HMI alarm list.
ctrlOpHmi@ABBRTU500	Control operations on the Integrated HMI: • View all configured Integrated HMI pages. • View and download process archive information in the HMI event list (events and indications, measured values and integrated total). • Acknowledge alarms in the HMI alarm list. • Do control operations in the Integrated HMI

Table 2: Account permissions available in the RTU

2.1.3 User roles

The user roles that group several account permissions could be changed according the needs. In delivery status the RTU500 series contains the following predefined user roles:

User role	Role explanation	Included permissions	Permission description
Viewer	Viewer	viewData@ABBRTU560	Read and view RTU data
Engineer	Engineer	viewData@ABBRTU560	Read and view RTU data
		config@ABBRTU560	Change configuration files
		firmware@ABBRTU560	Change firmware files
		enableTest@ABBRTU560	Enabling and use simulation and test mode
		enablePlc@ABBRTU560	Enable and use PLC online debug mode
		onlinePara@ABBRTU560	Online parameter changes
		onlineConf@ABBRTU560	Online configuration changes
Installer	Installer	viewData@ABBRTU560	Read and view RTU data
		config@ABBRTU560	Change configuration files
		onlinePara@ABBRTU560	Online parameter changes
Administrator	Administrator	usrAccount@ABBRTU560	User account management
		viewSecEvent@ABBRTU560	View security event logging / audit trails
		usrRole@ABBRTU560	User role management
Operator	Operator	viewData@ABBRTU560	Read and view RTU data
		viewDataHmi@ABBRTU560	Read/view data Integrated HMI
		ctrlOpHmi@ABBRTU560Sec	Control operations Integrated HMI
SECAUD	Security auditor	viewSecEvent@ABBRTU560	View security event logging / audit trails
SECADM	Security administrator	usrAccount@ABBRTU560	User account management
RBACMNT	Role based access control management	viewSecEvent@ABBRTU560	View security event logging / audit trails
		usrRole@ABBRTU560	User role management

Table 3: Default user roles in the RTU

During migration from the previous RTU560 user account management (before release 12) certain rules apply to convert to the new user roles defined above. These migration rules are:

- Existing user roles (default roles or new created roles) are kept, if there is any user assigned.
- The new user roles Engineer, Installer, SECAUD, SECADM and RBACMNT are added to the role definition, if not existing. The new roles get the account permissions as defined in the table above.

- If the user role System Engineer from a former UAM implementation exists, the account permissions onlinePara@ABBRTU560 (Online parameter changes) and onlineConf@ABBRTU560 (Online configuration changes) are assigned to this role.
- The account permission userRole@ABBRTU560 (User role management) is assigned to the existing user role Administrator. The user role Administrator must exist during migration, because it is not removable.

2.1.4 Local user accounts

The local user account representing a person is identified by a user name and a password. User name and password are free of choice within defined rules. See chapter "Password policies" for detailed information about the explicit and implicit rules for user names and passwords. The maximum number of different local user accounts in the RTU500 series is 100.

Each local user account can be assigned to one or more user roles with different account permissions. During an online connection with the RTU500 series Web server the user has to select a role from his assigned user roles. The user role can be changed during the online connection but at one point in time the user has one role with the defined account permissions, only. After login the changeable default user role is selected for a user.

In delivery status the RTU500 series contains the following predefined local user accounts, with their assigned user roles and their defined default user role:

Default user name	Default password	Assigned user roles	Default user role
Show	Show	Viewer	Viewer
Load	Load	Installer	Installer
Control	Control	Installer Engineer	Installer
Admin	Admin	Engineer Administrator	Engineer
Operator	Operator	Operator	Operator
Default	Default	Viewer Operator Installer Engineer SECAUD RBACMNT SECADM Administrator	Viewer

Table 4: Default user accounts in the RTU

During migration from the previous RTU560 user account management (before release 12) the existing local user accounts are taken as they are. That means user names, passwords and role assignments remains unchanged after the migration.

ADVICE

The predefined superuser Default is added to the local user accounts during migration from the previous RTU560 user account management. So, if the local user accounts are defined individual be sure to remove the superuser after the migration.

2.1.5 Password file

All information about account permissions, user roles and local user accounts are stored in a password file on the memory card (CompactFlash® or SD card) of a CMU. Several protection schemes are implemented to inhibit reading of the password file information. The handling of the password file within the RTU500 series is shown in figure below.

The RTU holds the password file in plain text in the RAM as central source. For the upload and download to the Web server the file is encoded with a symmetric key A provided in the RTU firmware. This allows exchange of the password file with other RTU's because the file can be decoded with the same key A in every RTU.

For storing on the memory card the password file is encoded with another symmetric key B calculated from the memory card id (serial number of memory card) and a hardware identifier. This key depends on the memory card and is individual per CMU. With this method the encrypted password file on the memory card cannot be copied to other CMU's or used for upload from the Web server.

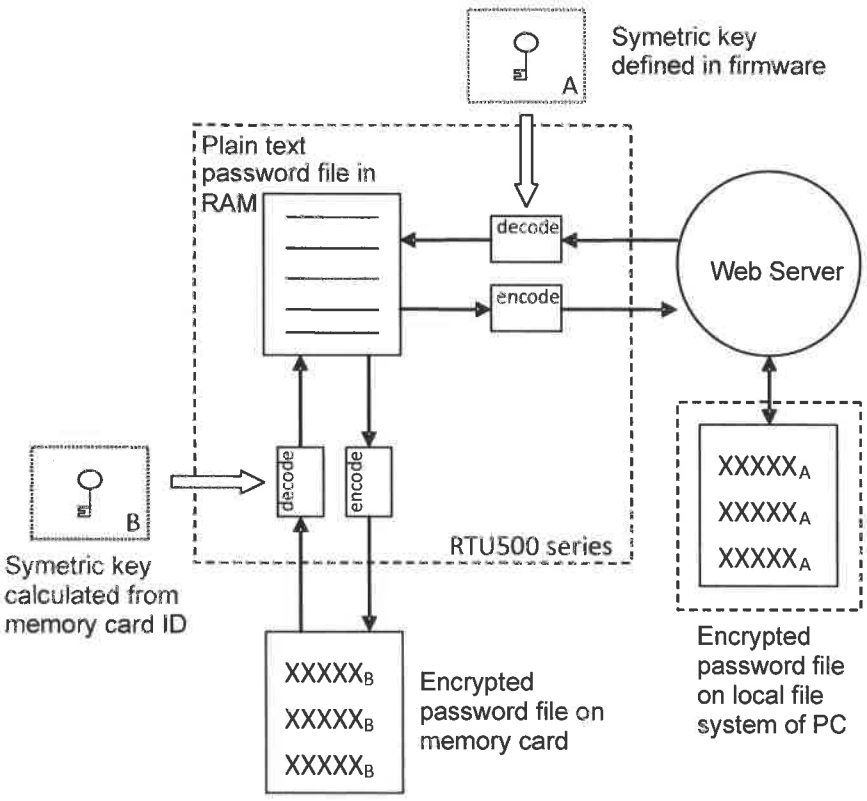


Figure 4: Encryption of password file

To compare the password files between different CMU's a SHA-256 hash value over the content of the password file is calculated and appended to the file (before encoding). During initialization the password file is decoded and the hash value is read.

For information exchange the different CMU's within a RTU560 communicate with each other. In case another CMU is detected during startup the password file hash value is requested from the other CMU. The received hash value is compared with the own value and in case of discrepancies the RTU goes to a restricted mode. In restricted mode all users are logged out and no access is possible anymore. The only available function is the possibility to harmonize the password files over all CMU modules. This function requires login as user with administrator permissions on all available CMU modules. For more information see chapter "Password file harmonization".

With the security enhancements beginning with release 10 the delivered memory cards contain a default password file encrypted with the specific key of the memory card. For updates of existing installation before release 10 a migration is possible. For this reason a migration flag is stored in the onboard flash on the CMU module. This allows detection whether a CMU module is started with the security enhanced firmware for the first time. In this case a default password file is created and stored on the memory card. With the migration flag stored on the CMU module it is not possible by the user to return to delivery status and reset the password file. The following figure shows the described migration concept. This concept applies for the migration to release 10 only. In higher releases the individual, encrypted password file exists already and there is no need to check the migration flag.

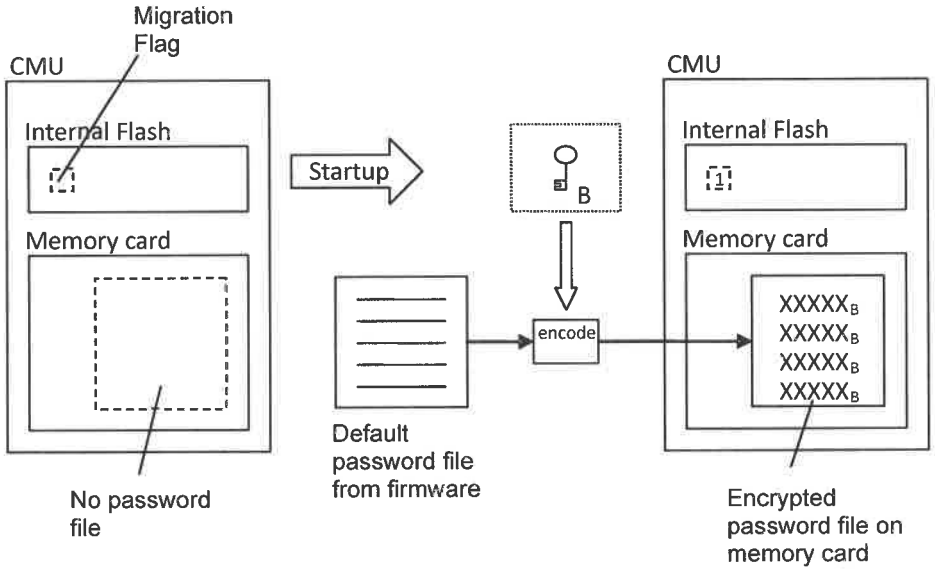


Figure 5: Migration of password file

If a CMU module is started without password file and set migration flag, no default password file is created and no login is possible via the Web server. This applies as well for a corrupted password file (e.g. because of unauthorized modification). In both cases the configured RTU functionality is still available but there is no access possible via Web server or Integrated HMI. A corresponding error message is shown to the user.

When password file is migrated the original password file is read and all defined users and roles are converted to the new account permission structure. The migration of users and roles is described in detail in the chapters above.

Besides the possibility to exchange the password file between different RTUs, the password file can be reset to the factory default. In this case all user accounts, user roles and password policies are reset to the default definition described in the chapters "Local user accounts" and "User roles".

2.2 User interface

2.2.1 RTUtil500 configuration

The security relevant configuration parameters are defined for a whole RTU. There is no configuration per CMU possible. The following parameters are configurable within RTUtil500:

- Maximum number of security events stored in the log. Configurable between 1000 and 10000 events with a default value of 3000.
- Timeout for automatic logout after user inactivity. Could be disabled and is configurable between 1 minute and 24 hours. Set to 60 minutes as default.

In RTUtil500 the security parameter are placed in the "Parameter" tap at an RTU (Network or Hardware tree). The figure below shows the RTUtil500 security parameter user interface.

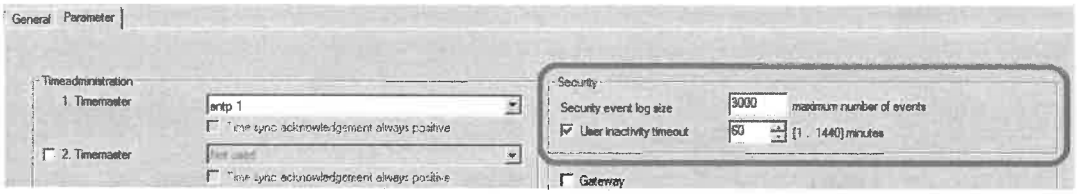


Figure 6: RTUtil500 security parameter user interface

2.2.2 User authentication

The information about the user authentication when accessing the RTU500 series Web server can be found in chapter "Web server user authentication". There the differences between the local and the central user account management regarding log-in are described.

2.2.3 Local user account management

All modification of local user accounts are done via the RTU500 series Web server. In the Web server menu the link "User Management" is the entry point for the local user account management. This link can be found under the menu item "Management" as shown in the figure below. Due to the sensible information in the user account management the following notice has to be considered.

ADVICE
The web pages of this functionality require secure HTTPS access. It is not possible to open the web pages with standard HTTP access.

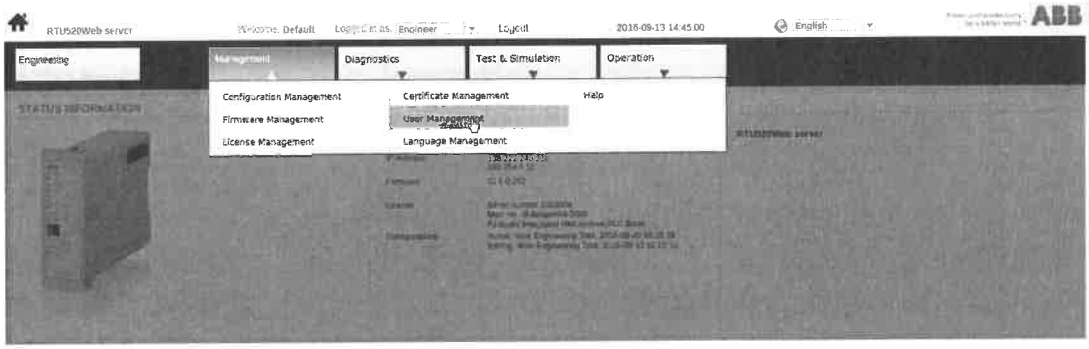


Figure 7: Web server menu user account management

The link starts a user interface to modify the following properties:

- Enable or disable functional policies
- Enable or disable password policies
- Add new or delete existing local user accounts
- Change user account passwords
- Add new or delete existing user roles
- Change assignments of user and permissions to/from user roles

The user interface for the account management consists of several menu tabs. The first 3 menu tabs cover the password policies, the local user accounts and the user roles. On each tab the corresponding information are shown for display and modification.

Common for all menu tabs are 2 buttons at the top of each tab. These buttons control the changes done by the administrator. At startup all control elements are disabled showing the current configuration. If changes shall be done the administrator just start to access the user interface. Then the both control buttons get active. After finishing the administrator can accept and store the changes by pressing the button "Save" or returning to the former configuration by declining the changes with the button "Cancel". It is irrelevant on which tab the control buttons are used. The change process could be started or finished on each tab.

ADVICE
Be sure to save any wanted modification in the user account management by pressing the "Save" button.

When the changes are accepted an additional dialog appears to confirm the decision. The changed account configuration is active right after accepting the changes. There is no need to reset the RTU but all users are logged out and a re-login is required. During accepting the changes are distributed within the RTU CMU's which could take a few seconds.

To avoid conflicts no access is possible via the Web server when an administrator has started the account change process. This compromises the access from other CMU's as well. The next chapters describe each menu tab in detail.

2.2.4 Security policies

In the first tab of the user management the security policies of the RTU500 series are defined. Security policies are general rules, which are valid for all users and for the whole RTU500 system. As shown in the figure below the security policies are divided into the following two sections:

- Functional policies that define restrictions in the access to the RTU500 series and
- Password policies that define rules that a password must fulfill to get accepted.

Figure 8: Menu tab security policies

The following sections describes the functional and password policies in detail.

2.2.4.1 Functional policies

The functional policies define restrictions in the access to the RTU500 series. When activated certain functionalities are disabled and cannot be used anymore. The following functional policies can be activated for the whole system:

- PLC online debugging
  Disable the access to the PLC online debugging. This includes start/stop of PLC programs, display and setting of PLC variables.
- COMPROTware RIO Server
  Disable the access to the COMPROTware RIO Server. That means disable the possibility to listening of telegram traffic on serial and Ethernet interfaces.
- Web server Test Mode
  Disable the Web server testing and simulation mode. This includes time administration, simulation of process inputs and commands in the test manager.
- Online parameter change
  Disable the possibility to change single parameters online with the Web server.
- Online configuration change
  Disable the possibility to change the RTU configuration online with the web server.

See part (1) of the Web server screen shoot "Fig. 8: Menu tab security policies" for the password policies user interface.

2.2.4.2 Password policies

The password policies define rules that a password must fulfill to get accepted by the RTU500 series. To enable the password policies the check box "Enforce password policies" must be checked (see figure in last chapter). Changes in the password policies are considered for new passwords only. That means existing passwords are not checked against the policies and the passwords are still valid and usable. To be sure that all passwords are compliant the passwords must be changed after defining a password policy.

After enabling the password policies the control elements are enabled and changes could be done. The following parameters are editable:

- Minimum length of a password. The required length of a password could be set to 0 which means no required length or to a value between 6 and 31. In case of 0 the password must be at least 3 characters long (see implicit rules below).
- Maximum lifetime of a password. This parameter defines the time after a password became invalid and could not be used anymore. The time is configured in days with a range from 0 to 1000. The value 0 means that the password never became invalid.
- Contains lower case characters. If this check box is set the passwords must contains at least one lower case character.
- Contains upper case characters. If this check box is set the passwords must contains at least one upper case character.
- Contains numeric characters. If this check box is set the passwords must contains at least one numeric character '0' to '9'.
- Contains special characters. If this check box is set the passwords must contains at least one of the listed special character:
  " [!£$%^&*@?<>+_]\"

Even when the password policies are not enabled there are certain rules for passwords. These are minimal rules to ensure proper system functionality. These implicit rules are:

- A password must be at least 3 characters long.
- A password must not be more than 31 characters long.
- A whitespace character is not allowed as part of the password.
- For passwords the following characters are allowed:
  "abcdefghijklmnopqrstuvwxyz"
  "ABCDEFGHIJKLMNOBQRSTUVWXYZ"
  "0123456789"
  "[!£$%^&*@?<>+_]\"

Independent from the password policies there are as well implicit rules for user names. These rules are:

- A user name must be at least 3 characters long.
- A user name must not be more than 31 characters long.
- A whitespace character is not allowed as part of the user name.
- For user names the following characters are allowed:
  "abcdefghijklmnopqrstuvwxyz"
  "ABCDEFGHIJKLMNOBQRSTUVWXYZ"
  "0123456789"
  "-.@_"

See part (2) of the Web server screen shoot "Fig. 8: Menu tab security policies" for the password policies user interface.

2.2.5 Local user accounts

In the second menu tab the local user accounts are defined. The tab shows in a table the names of the existing local user accounts (see figure below). The password of a user account can be changed by selecting the lock symbol at the left side of the table and by selecting the trash can symbol the local user account can be deleted. Be careful, there is no security query when deleting a local user account and a once deleted user account could not be restored.

On the right side of the table are the assignments of the user roles. One or several roles can be assigned to a local user account. The user role can be assigned or withdrawn by selecting the corresponding checkbox at the user account. The specific permissions assigned to a user role are defined in the menu tab "User Roles" described in the next chapter.

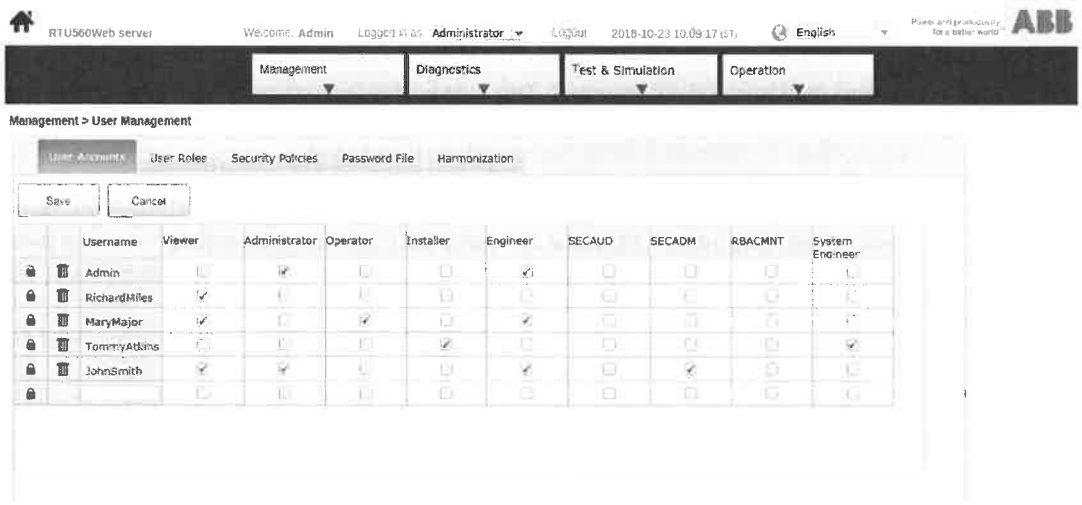


Figure 9: Menu tab user accounts

At the end of the table of existing local user accounts there is an empty field for adding a new local user. A new local user account is created by typing a user name and pressing <ENTER>. Then a dialog appears to set the initial password of the new user account (as shown in the next figure). By confirming the dialog with "Ok" the user account is created. For information about rules that must be consider when choosing a user name or password see chapter about the password policies.

When changing a local user password the same dialog appears as when setting the initial password. In the dialog the affected user name is displayed and 2 text fields to type the new password. The password must be typed two times to eliminate, unintentional typing errors. The new password is accepted only if both text fields contain the same password.

The new password is checked against the policies rules when the button "OK" is selected. In case of violations the password is declined, an error message is shown and a valid password must be defined. The dialog can be finished by pressing the button "Cancel". In this case the password is not changed and the old password is still valid.

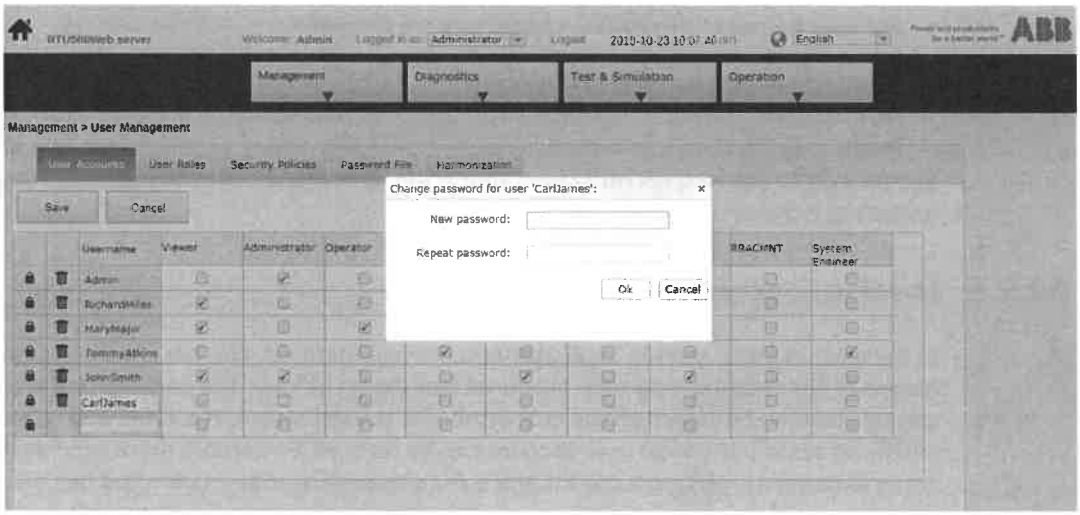


Figure 10: Dialog to change the password of a user

The Administrator can change the passwords of all local user accounts. A normal user can change the own password, only. To change the own password the user must select the tab "User Accounts" in the user account management. In this case the user account table shows

the logged in user and the password can be changed by selecting the lock symbol. In the change password dialog the current and the new password must be typed. By pressing "Ok" the minimum password policies are checked and if the password is valid the dialog closes. But closing the dialog does not store the new password on the RTU500 series.

To store the new password the button "Save" must be selected. With this step the new password is checked against the local defined policies rules and stored when valid. By pressing the button "Cancel" the password is not changed and the old password is still valid. The following figure shows the user interface for changing the own password of a CAM user.

Figure 11: Dialog to change the own password of a LAM user

2.2.6 User roles

In the third menu tab the user roles and there permission assignments are defined. The tab shows in a table the names of the existing user roles (see figure below). A user role can be deleted by selecting the trash can symbol on the left side of the table. Be careful, there is no security query when deleting a user role and a once deleted role could not be restored.

On the right side of the table are the specific permissions assigned to a user role. A permission can be assigned or withdrawn by selecting the corresponding checkbox at the user role.

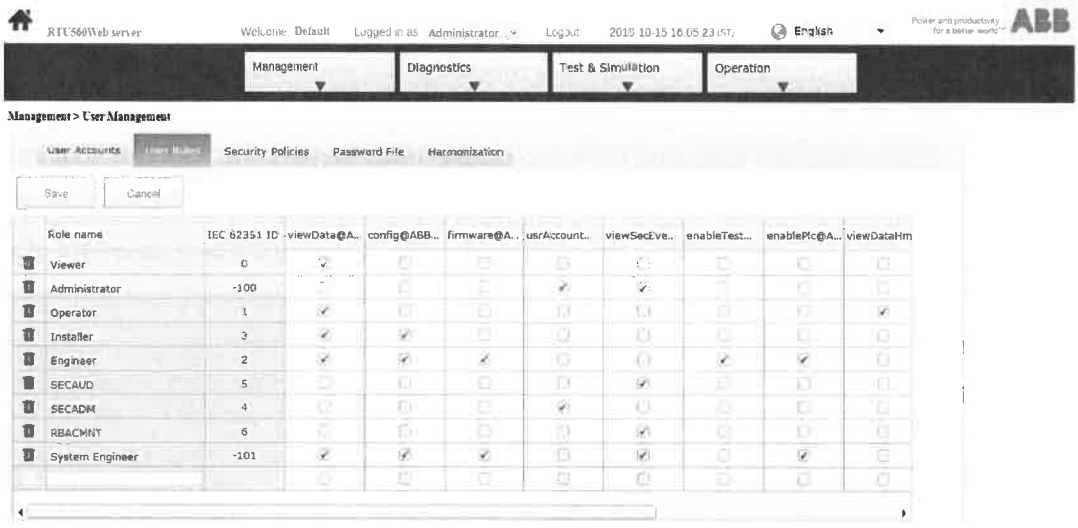


Figure 12: Menu tab user roles

There is an empty field at the end of the table of existing roles for adding a new user role. A new user role is created by typing a role name and pressing <ENTER>. There are the following rules defined for role names:

- A role name must be at least 3 characters long.
- A role name must not be more than 19 characters long.
- Whitespace characters are allowed as part of the role name
- For role names the following characters are allowed:
  "abcdefghijklmnopqrstuvwxyz"
  "ABCDEFGHIJKLMNOBQRSTUVWXYZ"
  "0123456789 "

For detailed information about the available account permissions see chapter "Account permissions".

2.2.7 Password file management

The password file of the RTU500 series can be reset to factory default and be exchanged between different RTUs. For this functionality the password file can be reset, uploaded and downloaded via the RTU500 series Web server. The corresponding user interface can be found under the link "User Management" in the menu item "Management". The figure below shows the user interface for the password file management in the tab "Password File".

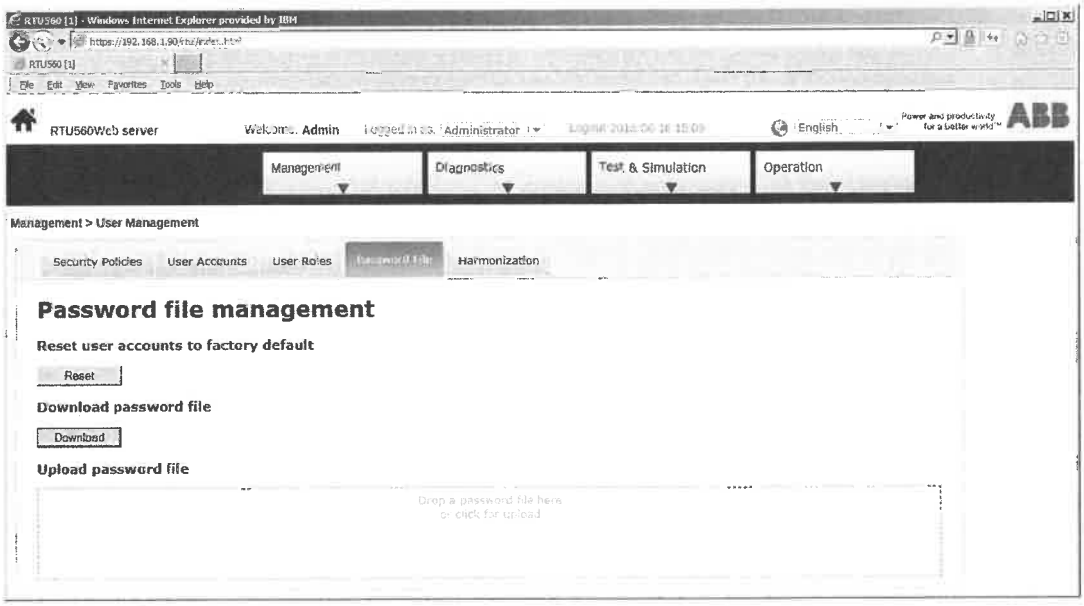


Figure 13: Menu tab password file management

To reset the password file to factory default the button "Reset" has to be used. When pressed a dialog appears to confirm the reset. After confirmation with "Ok" the default password file is active directly. A reset of the RTU500 series is not necessary, but all users are logged out and a re-login is required. After the reset all user accounts and passwords are reset to the default values. That means the re-login must happen with a default user and password.

For the exchange of a password file the file must be downloaded from an RTU first. This is done by selecting the button "Download" in the tab "Password File". When pressed an information status bar appears like shown in the figure below. To save the downloaded password file on the host PC select the button "Save".

Figure 14: Download password file

To upload a before downloaded password file on another RTU the file can be dropped to the dotted area shown in the figures above or the area can be clicked with the mouse. In the second case a file select dialog appears to choose the password file to upload. In both

cases a confirmation dialog appears to confirm the upload. After confirmation with "Ok" the existing password file is replaced by the uploaded file. If successful, the new password file is active directly. A reset of the RTU500 series is not necessary, but all users are logged out and a re-login is required.

2.2.8 Password file harmonization

In case the password file is inconsistent between different CMU's the RTU500 series goes into a restricted mode. In this mode a login is possible but the only function available is the harmonization of the password file. The harmonization of the password file requires administrator permissions. In restricted mode the Web server shows after login without administrator permissions the error message displayed below.

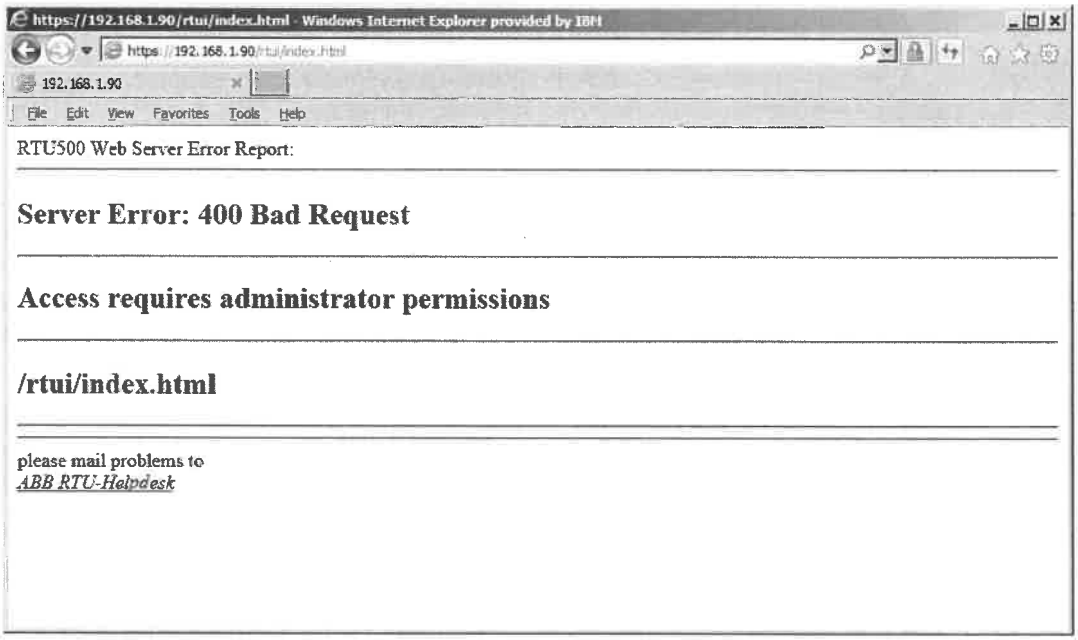


Figure 15: Error message administrator permissions required

ADVICE

Be sure to disable the advanced option "Show friendly HTTP error messages" if the Microsoft Internet Explorer is used as Web client. Without this option the detailed error information of the RTU500 series Web server are not shown. The option can be found in the "Advanced" tab of the "Internet Options".

After login with administrator permission the RTU500 series Web Server shows the normal user interface. But due to the restricted mode each function, besides the harmonization of the password file, is locked. If a locked function is selected the Web server shows a corresponding error message, like shown in the next figure.

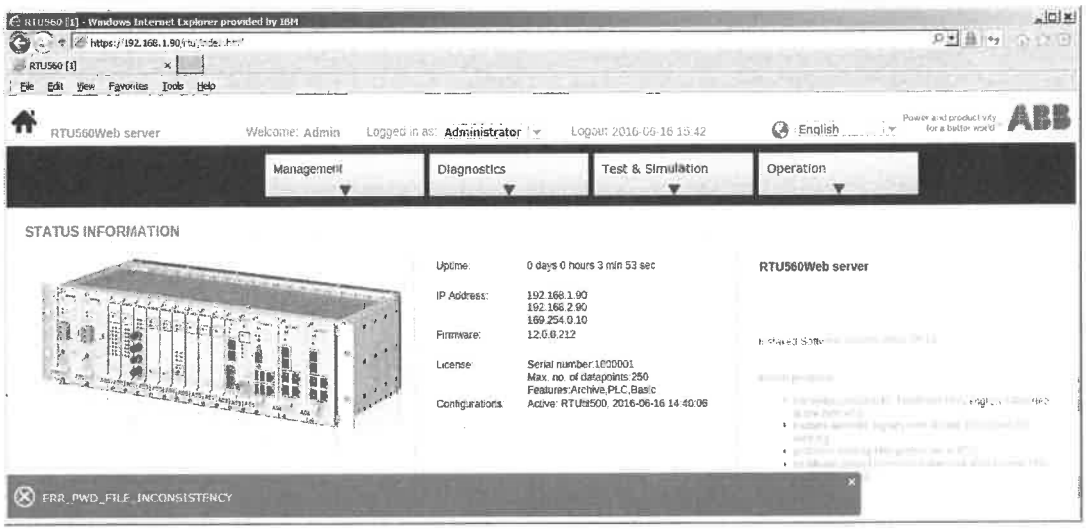


Figure 16: Error message password file inconsistency

To start the password file harmonization the link "User Management", found under the menu item "Management", must be selected (see figure below). When selected the user interface for the account management appears. The last tab (called "Harmonization") in the user interface is used for the password file harmonization by authenticate all available CMU's. Due to the sensible information in the authentication the following notice has to be considered.

ADVICE

The web pages of this functionality require secure HTTPS access. It is not possible to open the web pages with standard HTTP access.

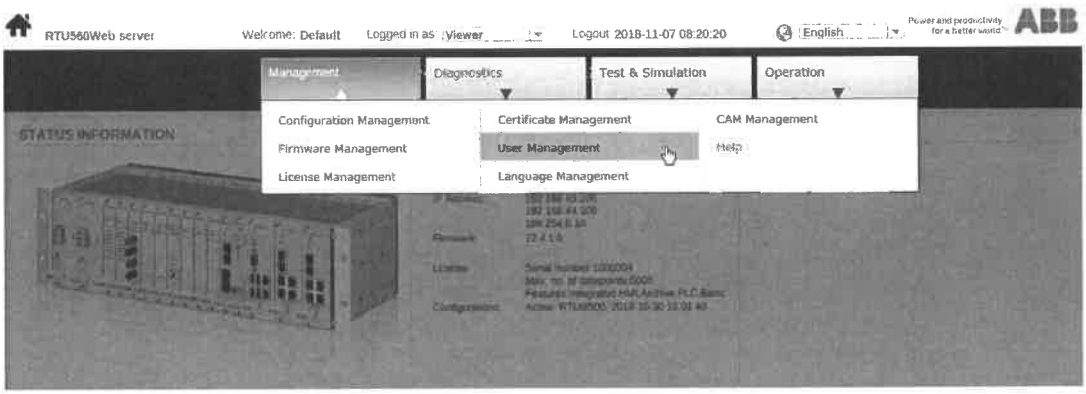


Figure 17: Web server menu user account management

Before a harmonization of the password file is possible, the authentication of the administration user must be provided by the user for all detected CMU's. The provided authentications are compared with authentications requested from the other CMU modules. Only if all authentications are correct the password file can be harmonized and distributed to the other CMU modules.

The next figure shows an example for an RTU with 2 CMU's. For each detected CMU the rack and slot address is shown. Furthermore there are input fields for user name, password and a button to authenticate each CMU. A CMU is authenticated by typing a user account with administrator permissions and selecting the button "Authenticate". A correct authenticated CMU is identified by the check box on the right side.

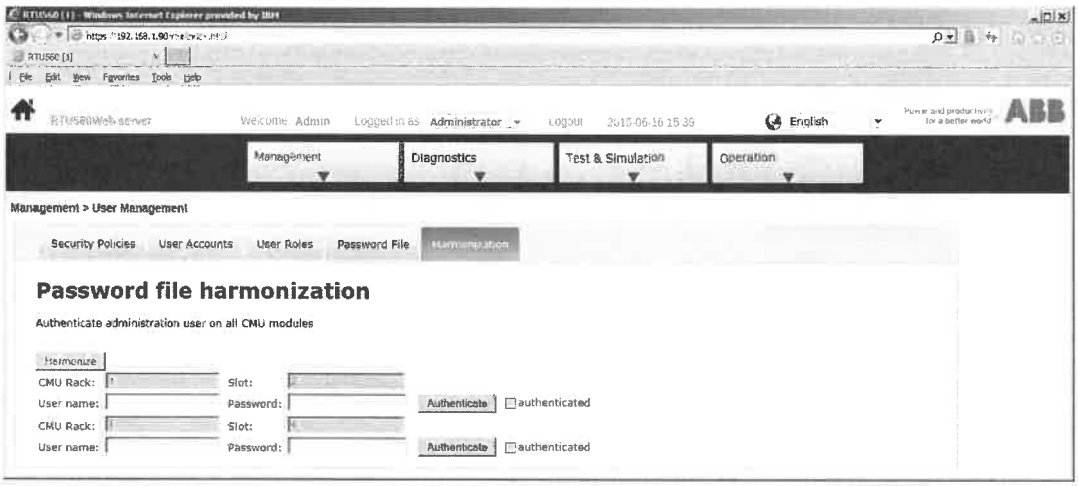


Figure 18: Password file harmonization

When all CMU's are authenticated the distribution of the password file is started by selecting the button "Harmonize" at the top of the page. The harmonization distributes the password file of the connected CMU to all other CMU's. The distribution within the RTU can take a few seconds. If the distribution was successful, the harmonized password file is active directly. A reset of the RTU500 series is not necessary, but all users are logged out and a re-login is required.

2.3 Recommendations

Recommendation	Implementation in the RTU500 series	Reference to standards
All default users and user passwords shall be deleted	The RTU system provides means to configure individual secure user accounts.	
There shall be individual user accounts. No shared user accounts shall be used.	The RTU system provides means to configure individual secure user accounts. Only with individual accounts the traceability in the security logs is possible.	
Users shall only have the minimum rights required.	The RTU provides a role based user account management. New roles can be defines. All predefined roles can be deleted.	
A strong password policy shall be defined.	Use the RTU password policy setting option to enable strong passwords.	• NERC CIP-007-3a "Cyber Security - Systems Security Management" • IEC 62443
A maximum lifetime for a user password shall be defined	Use the RTU password policy setting option to enable a password lifetime.	• NERC CIP-007-3a "Cyber Security - Systems Security Management" • IEC 62443

Table 5: Recommendations for local user account management

ADVICE

When removing user accounts or roles the RTU500 series firmware ensures that at least one administrator account remains (user account with permission "account@ABBRTU500"). Be sure to keep the password of this administrator account because there is no possibility to reset an administrator password. If the administrator password is lost, a new flash card (with factory settings) has to be used.

3 Central user account management

The central user account management (CAM) in the RTU500 series is an extension of the local account management (LAM) described in chapter "Local user account management". In a CAM setup the user authentication (with user name and password) is done on an external CAM server that manage all user accounts of a system. The authorization of a user via permissions assigned to user roles is still performed locally with the definitions in the LAM. That means there is a bisection between CAM and LAM and both functionalities must be considered when using a central user account management.

The communication between the RTU and the CAM server is done with the Lightweight Directory Access Protocol (LDAP). For CAM the RTU500 series supports the following server types:

- ABB IEC 62351 Authentication Server (integrated in SDM600)
- Microsoft Active Directory Server
- Group Based LDAP Authentication Server

For detailed information about the supported CAM server types see the following documentation links:

- For the ABB IEC 62351 Authentication Server
  System Data Manager SDM600 - User Manual
- For the Microsoft Active Directory Server
  Microsoft Active Directory Domain Service Documentation
- For the Group Based LDAP Authentication Server
  OpenLDAP project and documentation

The following chapters describe first the design principles and later the configuration to setup a central user account management in the RTU500 series.

3.1 Design principles

3.1.1 Account information

In a CAM setup the differentiation between user accounts, user roles and account permissions are the same as written in chapter "Account information" of the LAM description. This applies as well for the relationship between user, role and permission. But in a CAM configuration the account information are stored and handled in different places as shown in the figure below.

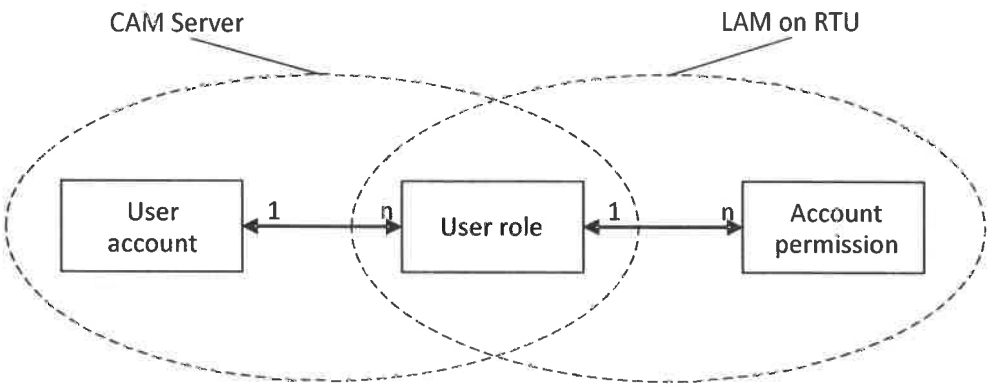


Figure 19: Division of account information between CAM and LAM

The user accounts and roles assigned to that user are stored and managed in the CAM server. The permissions assigned to user roles are stored and handled in the LAM of the RTU. The intersection between CAM and LAM is the user roles. This requires that user roles on the CAM server are defined in the same way as in the LAM of the RTU. A detailed description about this requirement can be found in chapter "User roles".

How the user accounts and roles are stored on the CAM server is outside the scope of this document. Please refer to the documentation of the used CAM server for more information about the storage of user accounts. The assignment of account permissions and user roles are stored on the RTU in a local password file (see chapter "Account information" of the LAM description).

3.1.2 Account permissions

As described for local account management (LAM), the account permissions available in the RTU500 series are fix defined and cannot be changed. This applies for central account management (CAM) setups as well. A detailed overview of all permissions and the allowed actions for every permission can be found in chapter "Account permissions" of the LAM description.

3.1.3 User roles

The user roles that group several account permissions are the boundary point between the central account management (CAM) server and local account management (LAM). In the CAM server roles are assigned to user accounts and in LAM permissions are assigned to user roles. For this task sharing the user roles on the CAM server must be defined in the same way as in LAM. To achieve this requirement the following rules must be considered depending on the used CAM server type.

With the ABB IEC 62351 Authentication Server the user roles are identified along the role id. The role id is specified in IEC 62351 for the standard and the user defined roles. The table shown below contains the role id definitions according to IEC 62351.

User role	Role explanation	IEC 62351 role id
Viewer	Viewer	0

Table 6: IEC 62351 user role ids

User role	Role explanation	IEC 62351 role id
Operator	Operator	1
Engineer	Engineer	2
Installer	Installer	3
SECADM	Security administrator	4
SECAUD	Security auditor	5
RBACMNT	Role based access control management	6
Administrator	Administrator	-100
<User defined role>	<User defined role>	-101 (decreasing numbered)

Table 6: IEC 62351 user role ids

For the standard roles from "Viewer" to "Administrator" the role ids are fix defined. This definition is used by the ABB IEC 62351 Authentication Server and the LAM on the RTU500 series. That means for the standard roles no adjustments has to be done with this CAM server type.

The user defined roles get a negative role id starting with -101 and are decreasing numbered. To get the same definition on the ABB IEC 62351 Authentication Server and the LAM the user defined roles must be created in the same order on the CAM server and the LAM. To check that ids of user defined roles are the same, the LAM shows the assigned role id in the user interface (see chapter "User roles" in the LAM description).

With the Microsoft Active Directory Server and the Group Based LDAP Authentication Server the mapping of roles between LAM and the CAM server is handled via the name of the role. This kind of CAM server doesn't support user roles but groups with a similar purpose. The user accounts on the CAM server can be part of one or more groups comparable to the user roles in LAM. To define a mapping between the groups and the roles, the naming of both must be the same like shown in the next table.

LAM user role name	Role explanation	CAM server group name
Viewer	Viewer	Viewer
Operator	Operator	Operator
Engineer	Engineer	Engineer
Installer	Installer	Installer
SECADM	Security administrator	SECADM
SECAUD	Security auditor	SECAUD
RBACMNT	Role based access control management	RBACMNT
Administrator	Administrator	Administrator

Table 7: Mapping between user roles and groups

This mapping of the standard roles from "Viewer" to "Administrator" is fix defined and cannot be changed. Be sure to create the groups in the CAM server with the same name as the standard roles in LAM. Additional groups not named as in LAM are ignored. So, user defined roles are not supported with the Microsoft Active Directory Server and the Group Based LDAP Authentication Server.

For all CAM server types the assignment of permissions to user roles can be changed in LAM according the needs. The predefined assignment of permissions in delivery status can be found in chapter "User roles" of the LAM description.

3.1.4 User authentication

For the user authentication a CAM client runs on the RTU that communicates with the external CAM server. The protocol used for communication is LDAP (Lightweight Directory Access Protocol) with additional TLS (Transport Layer Security) extension. The next figure shows the CAM authentication process in a functional overview.

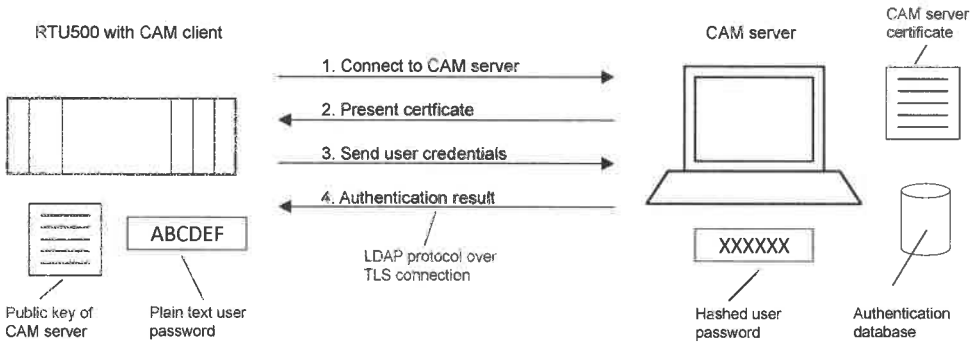


Figure 20: CAM user authentication process

The different steps to authenticate a user are:

1 As there is no permanent connection to the CAM server, the CAM client in the RTU begins by connecting to the server using the LDAP protocol. Within this step Transport Layer Security (TLS) is established on the connection to provide data confidentiality.
2 As response the CAM server presents for identification his certificate to the RTU. The RTU validates the certificate with the pre-loaded public key of the CAM server.
3 Afterwards the RTU sends the user credentials to the CAM server. In this step the RTU sends the user password as plain text (over the secure TLS connection of course). The reason for the plain text is the authentication data base on the CAM server. In this database the user passwords are stored as hashed values. But the parameters of the hash (algorithm, salt etc.) are not known by the CAM client. So the passwords have to be sent as plain text to allow hashing and comparing on the CAM server.
4 In the last step the CAM server compares the received user credentials with his database and sends the result of the authentication back to the RTU. Finally the connection to the CAM server is closed.

Besides the user authentication with the CAM client, the local account management can be used as backup. In this optional configuration LAM is used for user authentication if there is no connection to the CAM server.

3.1.5 CAM server public key certificate

To ensure the identity of the CAM server the RTU500 series validates the presented end-entity server certificate with the prior uploaded public key (see chapter "User authentication"). How the CAM server certificate is generated and signed depends on the server and is not part of this document. Please refer to the CAM server reference documentation (found here "Central user account management") for more information about the specific server certificate.

For the public key certificate uploaded to the RTU500 series the following issues has to be considered:

- The public key certificate can be extracted from the end-entity CAM server certificate. How this is done depends on CAM server. Appendix "A.1 Export CAM server public key certificate on Windows" shows an example for the Microsoft Windows certificate store.
- The public key certificate must contain the complete certification path. Make sure to extract the whole certification path, when creating the public key certificate from the end-entity CAM server certificate. Without the certification path the public key certificate is rejected as self-signed.
- The subject alternative name or the common name of the CAM server certificate must contain the IP address of the CAM server. This IP address is checked by the RTU500 series during the certificate validation.
- For uploading the public key certificate must be in PKCS#7 format with the file ending ".p7b".

The upload of a public key certificate is done via the RTU500 series Web server. For detailed information about the upload process see chapter "Certificate upload". When the upload is finished the public key certificate is active and can be used directly. A restart of RTU500 series device is not required.

3.1.6 CAM integration

In the RTU500 series with Central User Account Management several additional information are required besides the standard configuration file and the local password file. These information are provided to the RTU by uploading defined files or by web server user interfaces. For a better understanding of the following description of configuration options and user interfaces, the figure below shows for the CAM integration all related files uploaded to or stored on the RTU.

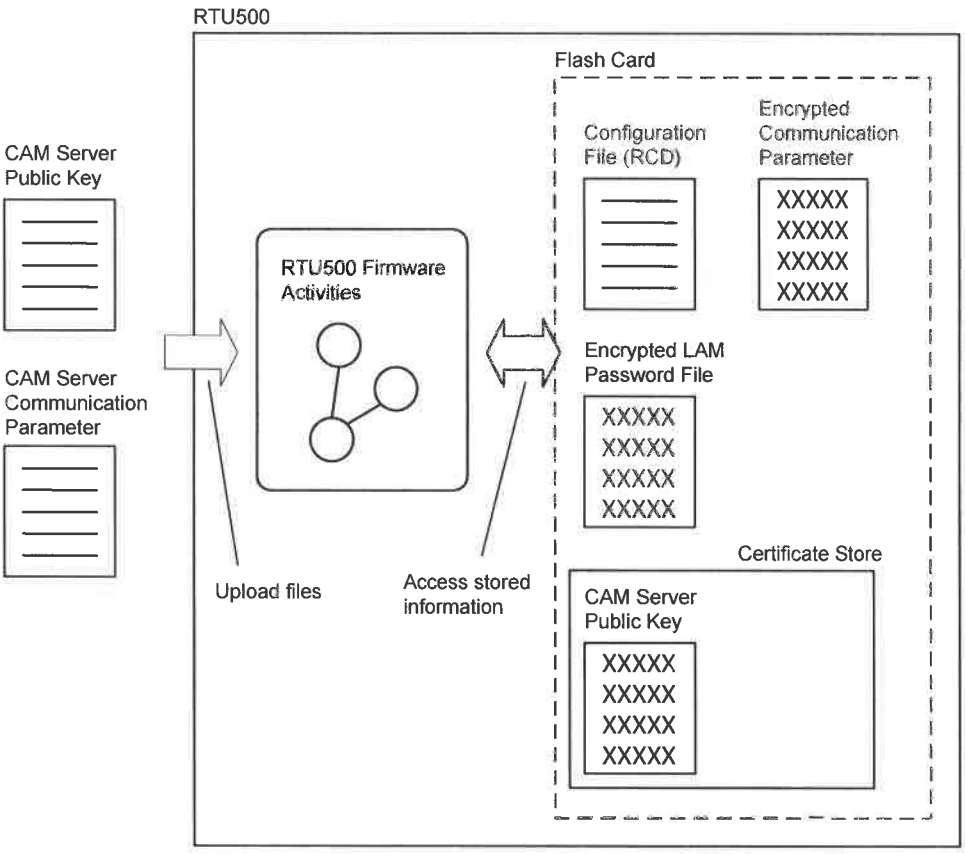


Figure 21: CAM related files in the RTU

The tasks of the different files are:

- CAM Server Public Key
  To authenticate the CAM server requested for user authentication the public key of the server is uploaded to the RTU. With the public key the certificate presented by the CAM server is verified to ensure the server identity. The uploaded public key is stored encrypted in the RTU500 series certificate store on the flash card.
- CAM Server Communication Parameter
  The communication parameters to access the CAM server (e.g. IP address of server) are not part of the RTUtil500 configuration. This is required to protect editing the parameters and to allow changes without updating the RTUtil500 configuration. The parameters can be configured by a corresponding GUI in the web interface or by uploading a structured text file containing these information. In both cases the communication parameter are stored encrypted on the flash card for subsequent access.
- Configuration File
  The standard RTU configuration file contains the basic CAM setup. This includes the CAM server type, the fallback options in case the CAM server is not available, the priority within the RTU in case of multiple CAM servers and the reference to the certificate store for uploading the CAM server public key.

- Local User Account Password File
  As described above the CAM servers covers the authentication of a user only. The authorization of a user is done with information in the local password file. That means whether a user is allowed to perform a certain action is not checked by the CAM server but by the role-to-permission assignments stored in the password file of the Local User Account Management (LAM). The assignment information can be set by a corresponding GUI in the web interface as explained in chapter "User roles" of the LAM description. The LAM password file with the role-to-permission assignments are stored encrypted on the flash card.

3.2 User interface

3.2.1 RTUtil500 configuration

To activate the central account management for the RTU500 series a CAM client must be added to the Ethernet interface of a CMU module. This is done in the hardware tree of the configuration tool RTUtil500. The figure below shows an example hardware tree with a CAM client added to the first Ethernet interface of a 560CMR02 CMU module. For more information about how to use and add functionality to the hardware tree in RTUtil500 please refer to the User Manual RTUtil500 Release 12 (1KGT 150 950).

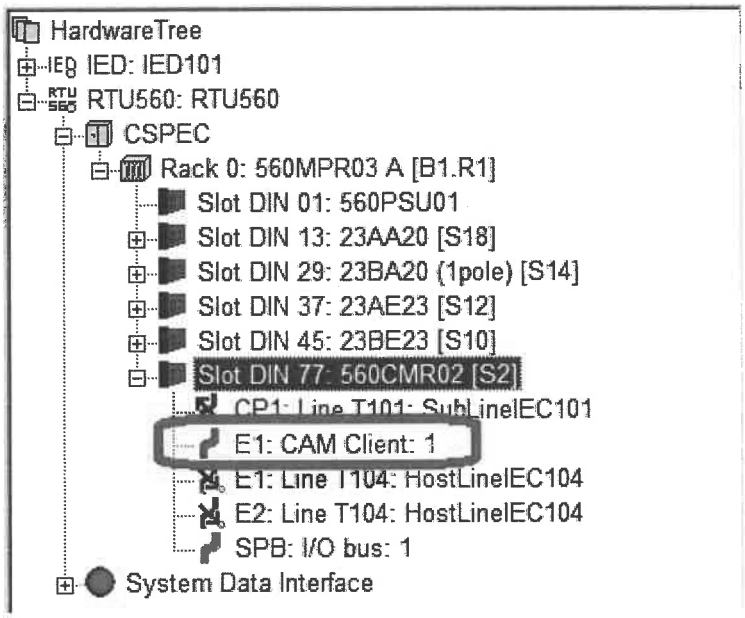


Figure 22: CAM client in hardware tree

For redundant setups multiple CAM clients can be configured within an RTU. The limits of multiple CAM clients are:

- Per CMU module 1 CAM client can be configured.
- Per RTU up to 4 CAM clients can be configured.

In multi CMU configurations, one CAM client on any CMU is sufficient to enable the CAM authentication for the whole RTU. CMU modules without CAM client are using the internal communication of the RTU to access the client on another CMU.

The CAM client in the RTU500 series access one logical CAM server that can consists of 1 or more physical machines. The communication parameters for the CAM server, like IP addresses or base distinguish names, are not part of the RTUtil500 configuration. These parameters

are set in the web interface as described in chapter "CAM management". The configuration options at a CAM client in RTUtil500 are shown in the next figure.

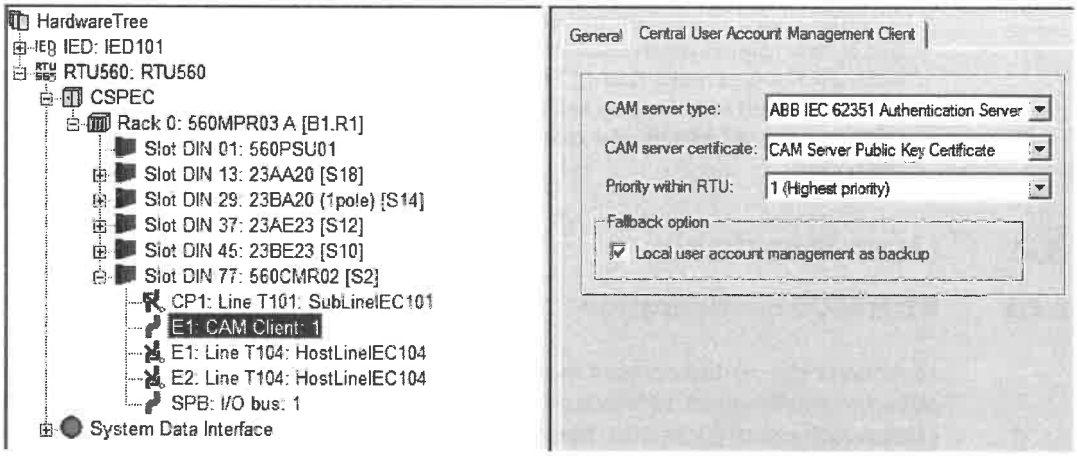


Figure 23: CAM client parameter in RTUtil500

In the RTUtil500 configuration the CAM server type, the CAM server certificate, the priority within the RTU500 and the fallback option has to be set.

As CAM server type the options “ABB IEC 62351 Authentication Server”, “Microsoft Active Directory Server” and “Group Based LDAP Authentication Server” are selectable. The CAM server type can be different for each CAM client within an RTU.

For the CAM server certificate, the certificate store has to be configured first. That means an entry has to be added to the certificate store representing the public key used to check the identity of the CAM server (see chapter "User authentication"). The certificate store configuration can be found in the hardware tree at the general tab of the CMU module (see next figure).

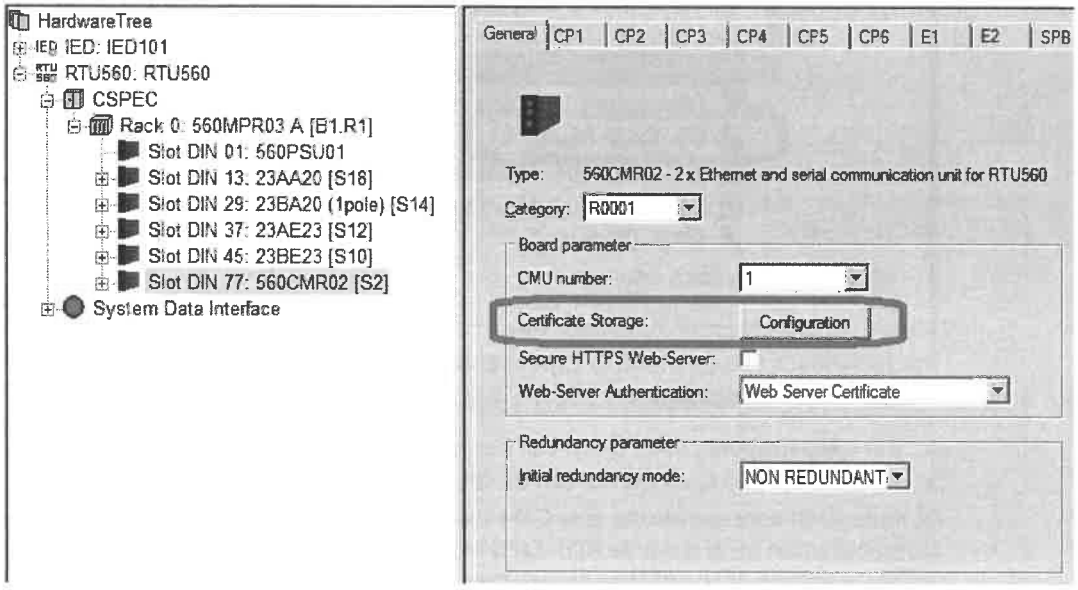


Figure 24: RTUtil500 certificate store configuration

The certificate store configuration opens by pressing the button "Configuration" shown in the figure above (near the text "Certificate Storage"). When selected a dialog appears with several entries for certificates. Each entry represents a certificate that shall be transferred to the CMU. To add a certificate, select the check box at the entry number and give the entry

a descriptive name. An example of the certificate store configuration is shown in the figure below.

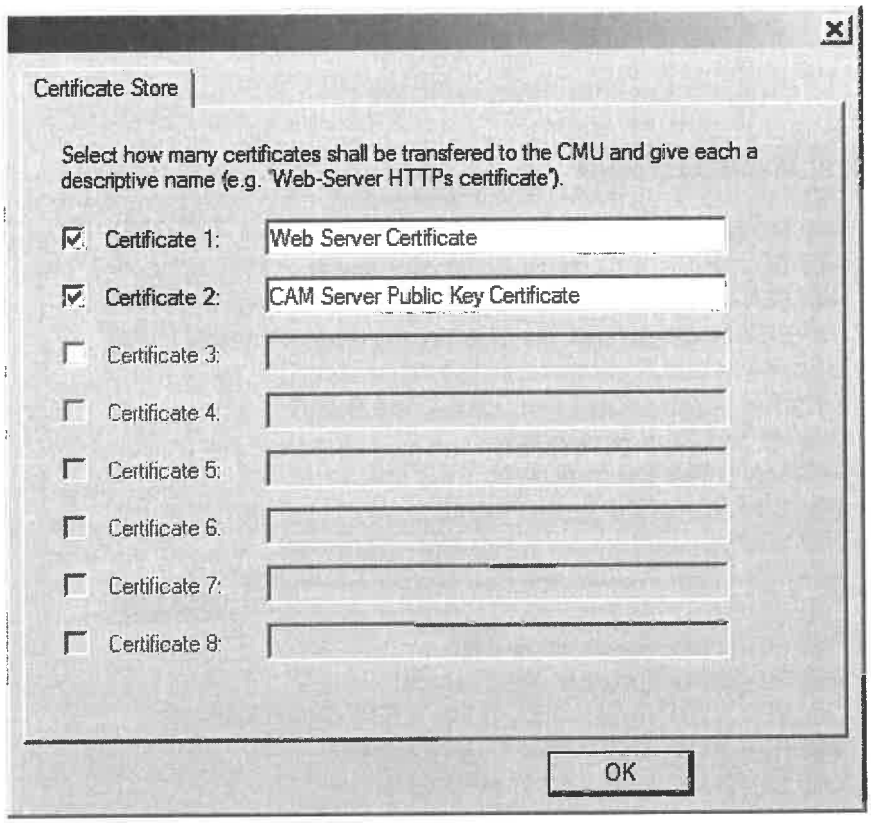


Figure 25: RTUtil500 certificate store

The priority of the CAM client is defined between 1 as highest priority and 4 as lowest priority. The consistency check validates as error whether each CAM client is configured with a different priority. The set priority is used as well to identify the system event (SEV) used to signalize the CAM server connection state (see below).

The fallback option when the connection to the CAM server is not available is the local user account management (LAM) with the local password file. The local password file used for LAM are not affected by the CAM client configuration. The password file remains on the RTU whether LAM is selected as fallback option or not. As described above, the password file is necessary because the included authorization information (role-to-permission assignment) is still required to validate the user actions.

To avoid unsecure configuration in connection with CAM please consider the following advice.

ADVICE
In a CAM configuration the user credentials are transmitted as plain text from the Web browser to the RTU500 series. Therefore the secure Web server access via HTTPS shall be enabled for the RTU500 series if a CAM client is used. This applies for all CMU modules in a multi CMU setup.

For each CAM client a system event signalize the state of the CAM server connection. The connection is checked on LDAP protocol level every 30 seconds. The system event is named "CAM client x online" like shown in the example figure below.

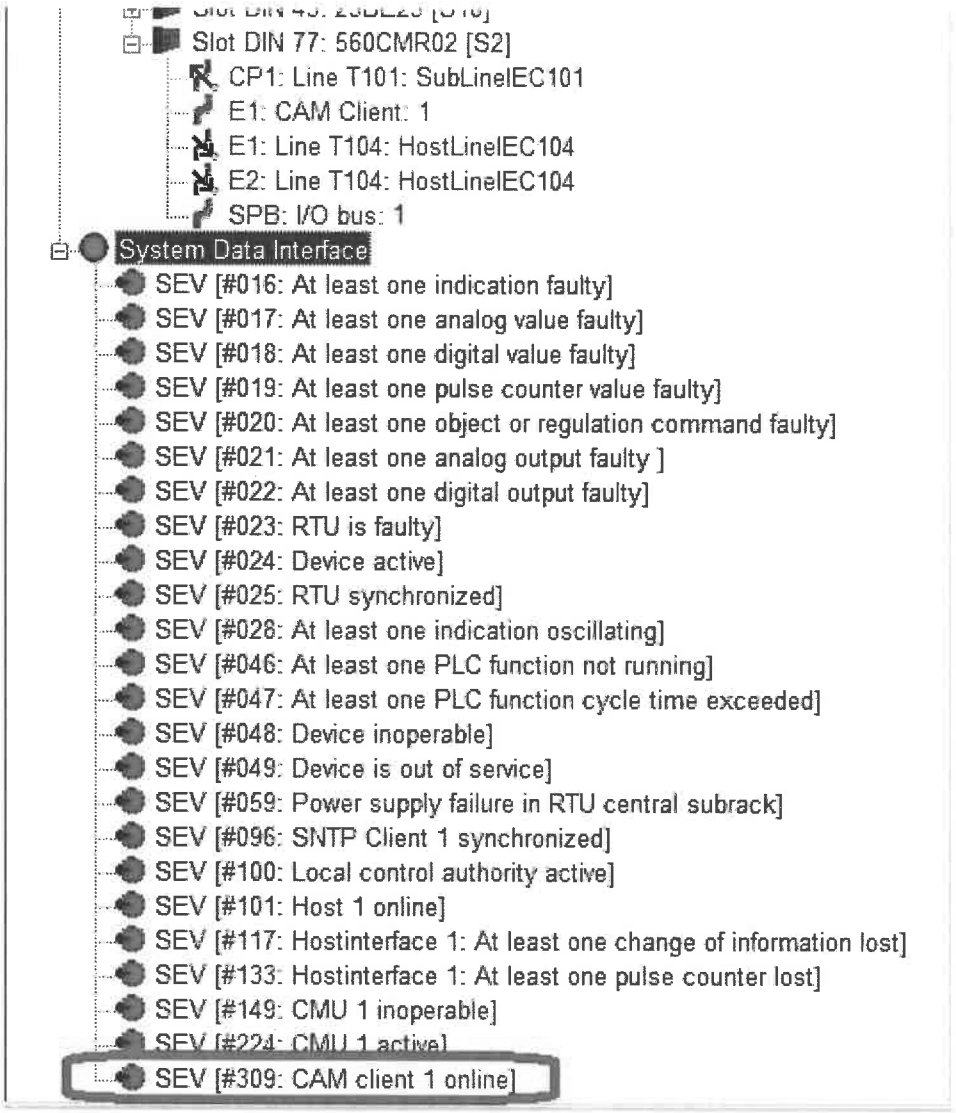


Figure 26: CAM client system event

3.2.2 User authentication

The information about the user authentication when accessing the RTU500 series Web server can be found in chapter "Web server user authentication". There the differences between the local and the central user account management regarding log-in are described.

3.2.3 CAM management

The central user account management (CAM) in the RTU500 series is enabled by an according configuration in RTUtil500. This configuration contains the type of CAM server but no communication related information. These information are set via the RTU500 series Web server to protect the access and to allow changes without updating the RTUtil500 configuration.

In the Web server menu the link "CAM Management" is the entry point for the communication configuration of the CAM client. This link can be found under the menu item "Management" as

shown in the next figure. The link is shown if no CAM client is configured, as well. In this case an error message appears if the menu item is selected.

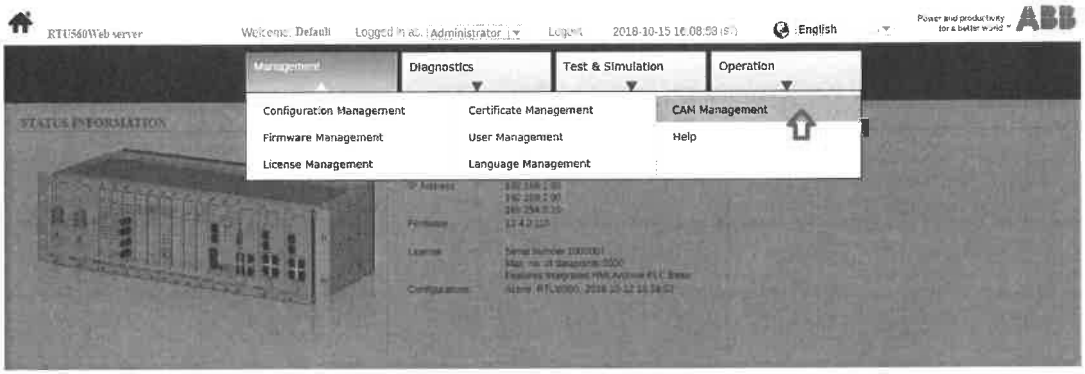


Figure 27: Web server menu CAM management

Selecting the menu item starts a user interface to perform the following tasks:

- Set the communication parameter of the CAM client
- Sending the communication parameter of the CAM client in a file to the RTU
- Receiving the communication parameter of the CAM client in a file from the RTU
- Activate or deactivate the CAM client
- Test the connection and authentication of the CAM server

The user interface for the central account management consists of several menu tabs. Each menu tab handles one (or more) of the tasks stated above. The next chapters describe each menu tab in detail.

The user interface is available on the CMU (none redundant CMU or active CMU of redundant pair) that contains the CAM client only and the configuration is specific for this CAM client. On other CMUs without CAM client (in a multi CMU setup), no information are shown in the CAM management user interface. That means the CAM client must configured on the CMU that contains the client.

Additional to the communication parameter the CAM server public key certificate must be uploaded to the RTU500 series. Information about the certificate for the CAM server can be found in chapter "CAM server public key certificate".

3.2.3.1 Setting communication parameters

In the first tab of the central user account management the communication parameter of the CAM client can be set. In a grid view information about the CAM client are shown and specific communication parameter can be set. An example of the user interface is shown in the figure below.

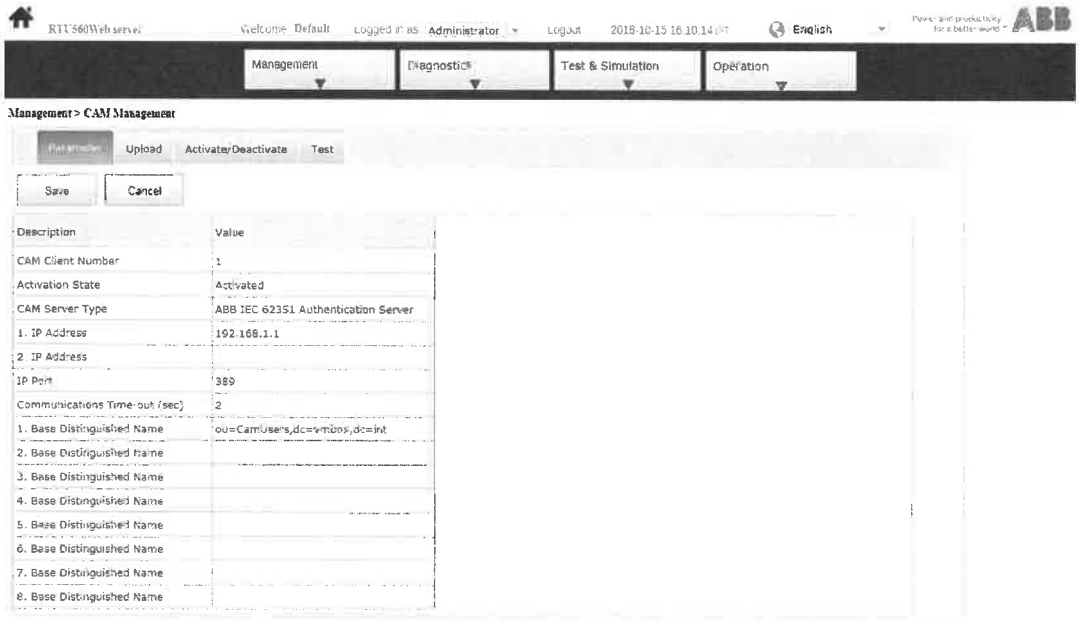


Figure 28: Menu tab for communication parameter setting

As information, the grid view shows the CAM client number, the actual CAM activation state and the CAM server type. The client number and the server type are from the RTUtil500 configuration used. The activation state indicates whether the specific CAM client is active or not. For detailed information about the possible activation states see chapter "Activate CAM client". The information part in the grid view is static and cannot be changed by the user.

The subsequent connection parameters can be set by the user or changed from the default values. The parameters are up to two IP addresses of the CAM server, the used TCP/IP port and the communication timeout in seconds. The timeout is required to consider low bandwidth connections.

Besides the connection parameters up to 8 base distinguish names (Base DNs) can be defined. The base distinguish names defines in which area/domain the CAM server shall search for the requested user authentications. The area/domain is a classification criterion not related to user groups or roles. Please refer to the documentation of the used CAM server to determine how the base distinguish names must be set.

Editing the communication parameters is possible if the CAM client is not active, only. If the client is active the parameters are shown but cannot be changed. To enable editing again the CAM client must be deactivated. When editing is finished the changes must be confirmed by pressing the "Save" button above the grid view. When saved the parameters are checked for validity and stored on the RTU. In case of invalid parameters an according error message appears and the parameters are set back to the last values. If the web page is switched without saving the communication parameters, any changes are lost.

If the parameter changes shall be dismissed and not stored on the RTU, the button "Cancel" can be pressed. In this case a confirmation dialog appears and if approved the last stored parameter are reloaded, overwriting any changes.

To be able to activate the CAM client in the RTU500 series the following communication parameters must be set at least:

- One CAM server IP address. The second IP address can be set for redundant server setups.
- The TCP/IP port. It is recommended to use the standard LDAP port 389 (default value) but this can be changed if required.

- The communication timeout between 1 and 300 seconds.
- At least one base distinguish name. The other distinguished names can be set if the CAM server shall search for users in several domains.

3.2.3.2 Upload communication parameters

In the second menu tab the communication parameter of the CAM client can be uploaded to or downloaded from the RTU. The CAM client communication parameters are included in a structured XML text file for upload and download. For uploading the RTU500 series supports 2 XML file formats. First the file format specified for the ABB Authentication Server included in SDM600 (SDM600 format). And second an extend format including all CAM client communication parameter supported by the RTU500 series (RTU500 format). For detailed information about the file formats see the paragraphs below.

The user interface for uploading and downloading the communication parameter (see figure below) are separated in two areas. The upper area contains the communication parameter actually stored on the RTU500 series and the lower area controls the uploading to the RTU.

Figure 29: Menu tab for upload/download CAM client communication parameter

To download the actual stored communication parameter press the receive button ( ) in the grid row for the communication parameter (in the upper area). When pressed the actual parameters are downloaded from the RTU and stored in XML format in the download folder of the host PC. The XML format used is the extend format including all CAM client communication parameter supported by the RTU500 series. The received file is a standard text file that can be edit and sent back to the same or any other RTU with CAM client. The name of the downloaded file is “camComConf.xml”.

To upload the CAM client communication parameter to the RTU, the following steps has to be executed in the lower area of the user interface:

1 Select in the column for the file description the "CAM client communication parameter". The both file formats supported by the RTU500 series are automatically detected.

2 Select a file with communication parameter by dropping the file on the lower area or by using the file open dialog that appears when clicked with the mouse. The XML parameter file must be in one of the both supported formats. The file to upload can have any name but the extension must be "*.xml".

When both steps are finished the communication parameter can be uploaded to the RTU by pressing the send button (see figure below). The send button doesn't appear before all required information are set. The uploaded file with the communication parameter are checked for completeness, validity and plausibility by the RTU500 series firmware. If the uploaded file is not correct the CAM client communication parameter are not set and an according message is presented to the user.

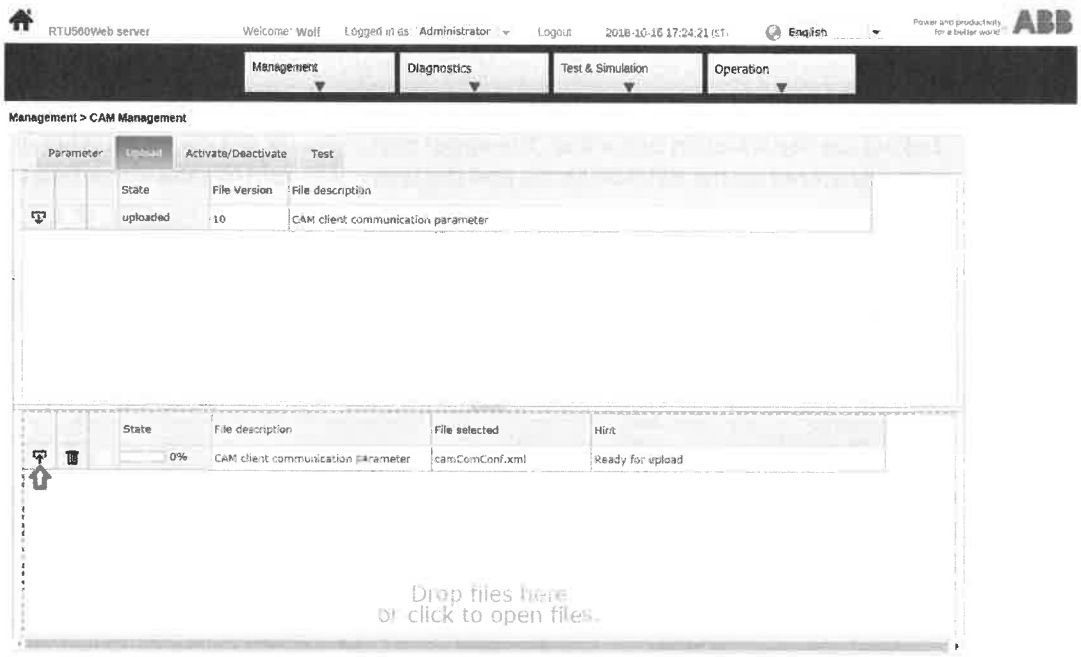


Figure 30: Example CAM client communication parameter upload

The version number shown in the upper area can be used to check whether different RTUs use the same CAM client communication parameter. The version number is build according to the following rules:

- When a parameter file in SDM600 format is uploaded to the RTU the version number is reset to 0. Because the SDM600 format doesn't contain a version information.
- When a parameter file in RTU500 format is uploaded to the RTU the version number is overwritten by the number stored in the file (see format below).
- Each time the communication parameter are changed and saved in the "Parameter" tab, the version number is increased by 1.

The both file formats supported for the communication parameters are the SDM600 and the RTU500 format. In both formats the parameters are described in an XML structure. The difference between the formats are the available parameters and the used XML tags. The RTU500 format contains all CAM client communication parameter supported by the RTU500 series including a version number. The SDM600 format contains besides other definitions a subset of the supported parameter only. The following section shows an example of the SDM600 format:

```
<?xml version="1.0"?>
<SDM600_CAM_IED_Configuration
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
 xmlns="http://abb.com/ConfigurationSchema.xsd">
  <IED_information>
    <name>Aeroglen</name>
    <description>Aeroglen</description>
    <address>192.168.0.110</address>
  </IED_information>
  <BaseDN>ou=CamUsers,dc=vmbox,dc=int</BaseDN>

<Replication_Group>memberOf=cn=RTU_Engineer,ou=Groups,dc=vmbox,
    dc=int</Replication_Group>
  <Replication_Interval>1440</Replication_Interval>
  <CAM_Servers>
    <CAM_Server>
      <ldapaddress> ldap://192.168.0.201:389</ldapaddress>
    </CAM_Server>
  </CAM_Servers>
</SDM600_CAM_IED_Configuration>
```

The parameters relevant for the RTU500 series in the SDM600 format are the base distinguish name "BaseDN" and the LDAP address "ldapaddress". The distinguish name is taken as it is and the LDAP address is parsed for the IP address and port number of the CAM server. The parameter file in SDM600 format are part of the configuration package generated by SDM600 (see System Data Manager SDM600 - User Manual). Before uploading the parameter file to the RTU extract the file from the configuration package (ZIP format) provided by SDM600. The file can be identified by the extension "*.xml".

The RTU500 format contains all communication parameter shown in the "Parameter" tab and described in chapter "Setting communication parameters". An example of the RTU500 format is shown in the next section.

```
<?xml version="1.0" encoding="UTF-8"?>
<rtu500CAMConfiguration version="12">
  <camServers>
    <camServer>
      <ipAddresses>
        <ipAddress>192.168.1.1</ipAddress>
        <ipAddress>192.168.2.1</ipAddress>
      </ipAddresses>
      <ipPort>389</ipPort>
      <comTimeout>2</comTimeout>
      <baseDNs>
        <baseDN>ou=CamUsers, dc=vmbox,dc=int</baseDN>
        <baseDN>ou=rtuUsers, dc=vmbox,dc=int</baseDN>
      </baseDNs>
    </camServer>
  </camServers>
</rtu500CAMConfiguration>
```

The parameter file in RTU500 format can be edit by the user or build from scratch with the needed values. Use the example above as guideline but do not exceed the maximum number of supported parameters. Two CAM server IP addresses and up to 8 base distinguish names are permitted. For uploading the parameter file to the RTU make sure the file name extension is "*.xml".

3.2.3.3 Activate CAM client

In the third menu tab the CAM client on the RTU can be activated or deactivated. When the CAM client is not active, which is the default state after the configuration, the user authentication is done with the local user account management (LAM). After the activation the user authentication is done on the CAM server. If the CAM server is not available LAM can be used as fallback, if configured accordingly (see chapter "RTUtil500 configuration"). The next figure shows the structure of the menu tab for activation/deactivation.

Figure 31: Menu tab for CAM client activation and deactivation

The user interface shows the buttons for activation and deactivation the actual activation state of the CAM client. The possible activation states are listed below:

- In Configuration
  This is the default state indicating that the communication parameters of the CAM client must be set or send to the device. The CAM client remains in this state as long the required communication parameter are not set and the CAM server public key certificate is not uploaded to the RTU. In this state the user interface shows (in this tab) a list of missing information and configuration mistakes that must be added or solved. Activation of the CAM client is not possible in this state.
- Ready for Activation
  When all required communication parameters for the CAM client are set and the CAM server public key certificate is uploaded the state change to "Ready for Activation". In this state the CAM client can be activated by pressing the button "Activate".
- Activated
  The state "Activated" indicates that CAM client is active and the user authentication is done on the CAM server. Activating the CAM client doesn't lead to log-out. That means the actual existing user session, whether the user is authenticated by LAM or CAM, remains and the user stays logged-in. When activated the CAM client can be deactivated by pressing the button "Deactivate".

The buttons for activation and deactivation of the CAM client are enabled according to the actual state. In configuration both buttons are disabled and cannot be selected. When the CAM client is activated the "Deactivate" button is enabled and if the state is "Ready for Activation" the button "Activate" can be selected.

3.2.3.4 Test connection

The last menu tab contains the user interface for testing the CAM server connection. The testing allows to check the communication setup without the necessity to log-off from the web interface. The test functionality allows to check the LDAP connection to the CAM server and as well the user authentication on the CAM server. The figure below shows the user interface for testing the CAM client.

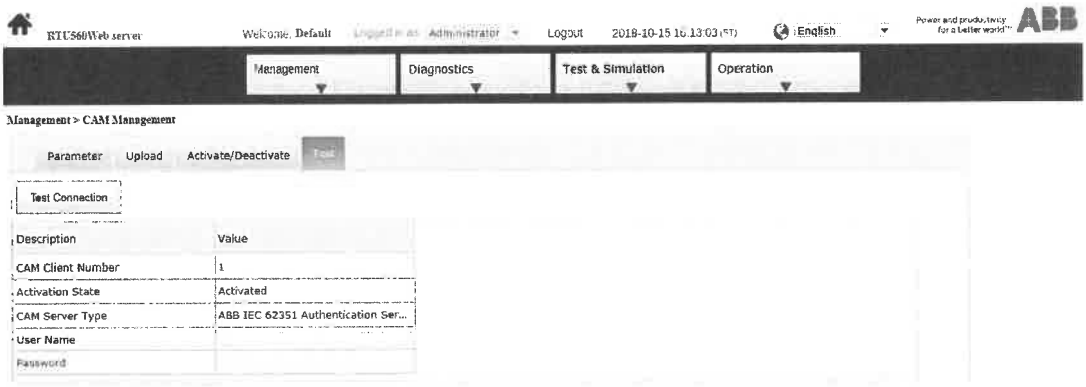


Figure 32: Menu tab for testing CAM server connection

Testing the server connection is only possible, if the CAM client communication setup is complete and the CAM client is active. If the client is not active an error message appears when the tests are executed. To start the tests follow the instructions below:

- Testing the LDAP connection
  For testing the LDAP connection to the CAM server the button "Test connection" must be pressed only. The result of the test is shown with an according message at the bottom of the browser window. This test doesn't check the uploaded CAM server public key certificate.
- Testing user authentication
  To test the user authentication provide a user name and password in the according input fields and press the button "Test connection". An according message at the bottom of the browser window shows the result of the test. This test covers the uploaded CAM server public key certificate. If the user name or the password is missing no authentication but the LDAP connection is tested, only.

As the CAM client must be active when performing the tests, be sure to consider the following advice.

ADVICE

If the user authentication test fails with a correct user name and password, deactivate the CAM client before checking for the reason. Because with activated CAM client and failed user authentication you may be excluded from the RTU500 series Web server.

3.2.4 Change user password

In the central account management all user accounts and their passwords are stored on the CAM server. The administrator of the CAM server can enforce the change of a user password by setting an expiration time for password. In this case the user must change his own password after the set time interval. This change can be down in the RTU500 series Web interface.

To change the own password the logged-in CAM user must select the menu tab "User Accounts" in the user account management. As for the local user accounts the appearing table shows the logged in user and the password can be changed by selecting the lock symbol. In the change password dialog the current and the new password must be typed. By pressing "Ok" the minimum password policies are checked and if the password is valid the dialog closes. But closing the dialog does not store the new password on the CAM server.

To store the new password on the CAM server the button "Save" must be selected. Then the new password is checked against the policies rules defined on the CAM server and stored

when valid. If changing the password succeeds the user is logged-out. If the new password is invalid or the current password is incorrect an according error message is shown. By pressing the button "Cancel" the password is not changed and the old password is still valid. The following figure shows the user interface for changing the own password of a CAM user.

Figure 33: Dialog to change own password of a CAM user

4 Security event logging

Security relevant user operations within the RTU are logged as security events in a file on the flash file system. A security event contains an event id (see chapter "Security event types"), a time stamp, a sequence number, the user name, the severity of the action and the name of the source.

Each CMU in an RTU has an own security event log. In every log the security events of the complete RTU are stored, but the event log is not equalized between different CMU modules. The content of security event log could be shown in the RTU500 series Web server. The events shown are from the CMU module the web server or integrated HMI is connected to.

To ensure integrity of the event log a salted hash value is calculated for the content of the log and stored together with file. During initialization of the RTU the event log is checked for integrity with the stored hash value. In case of differences a diagnosis log entry is created and a corresponding event is written to the log.

The security events logged in an RTU can be sent to external security log servers. The RTU supports the protocols Syslog UDP, Syslog TCP and ArcSight TCP for external log servers.

4.1 Security event format

The security events in the RTU500 series have a fix format. This format could not be changed and contains the following attributes:

- Sequence number
- Time stamp with time and date
- Name of user that causes the event
- Event id representing a certain event type (see next chapter)
- Severity of the event. Possible value are "Event" and "Alarm" depending on the importance of the event
- Source of the event. Defined as name of the RTU taken from the configuration.
- Event text that's describes the user operation (fix per event type)
- Additional, changing information text (variable per event type)

4.2 Security event types

The RTU500 series supports a defined set of security event types. Each type is identified by a unique event id. The following list summarizes the supported event types.

Event id	Event name	Comment
1110	Log-in successful	Log in via Web server or Integrated HMI
1120	Log-in failed - Unknown user	Reason logged but not shown as error message
1140	Log-in failed - Wrong password	Reason logged but not shown as error message
1150	Log-in failed - Password expired	Logged and shown as error message
1170	Log-in failed 3 times	

Table 8: Security event types in the RTU

Event id	Event name	Comment
1210	Log-out (user logged out)	
1220	Log-out by user inactivity (timeout)	Timeout configurable
1370	Viewed Security Event logs successfully	
1670	Viewed security event list failed	
1720	User Accounts reset to factory default	
2110	User account created successfully	
2120	User account deleted successfully	
2130	User account creation failed	
2140	User account deletion failed	
2160	New role assigned to user successfully	
2162	Permission added successfully	Permission assigned to role successfully
2170	User role assignment removed successfully	Role withdrawn from user successfully
2172	User permission removed successfully	Permission withdrawn from role successfully
2180	New role created successfully	
2190	Role deleted successfully	
2210	User password changed successfully	Own password only or administrator permissions required
2220	Change of user password failed	Own password only or administrator permissions required
2230	New user role assignment failed	Assigning role to user failed
2232	Addition of permission failed	Assigning permission to role failed
2233	User Password change failed - too short	
2235	User Password change failed - policy check failed	
2240	User session role changed successfully	
2245	User session role change failed	
2270	Role assignment removal failed	Withdraw role from user failed
2272	User permission removed failed	Withdraw permission from role failed
2280	New role creation failed	
2290	Role deletion failed	
2510	Password file on CF card corrupted	
3210	TCP communication with security log subscriber failed	
3220	Log data hash check failed (Log data altered)	Security event log was modified or deleted
3430	Security log file deleted by system	Migration to new version or log modification
3710	CAM Server communication successful	
3810	CAM Server communication failed	
4310	VPN Connection successful	

Table 8: Security event types in the RTU

Event id	Event name	Comment
4350	VPN Connection failed - Negotiation failed	
5110	Manual Reset	Restart via Web server
5160	Gateway/RTU restarted	Power off or restart via Web server
6110	Test Mode started	Allow simulation via Web server
6120	Test Mode ended	Permit simulation in Web server
6130	Control operation performed successfully	Logged once in test mode
6132	Failed to perform a control operation	Logged once in test mode
6140	Signal forced - value changed	Logged once in test mode
6210	System time set manually successfully	System time set via Web server
6310	System time set manually failed	
6510	Debug mode started successfully	PLC debug mode
6520	Debug mode ended	PLC debug mode ended manual or by timeout
6550	Protocol logging mode started	RIO protocol logging
6560	Protocol logging mode ended	RIO protocol logging ended manual or by timeout
8030	New certificate generated successfully	
8230	New certificate generation failed	
13200	Configuration transferred to the device successfully	Covers all kind of configuration files
13220	Configuration changed successfully	Online configuration via Web interface
13250	Entered configuration mode successfully	Online configuration via Web interface
13260	Exited configuration mode successfully	Online configuration via Web interface
13300	Configuration files read/exported from the device successfully	Covers all kind of configuration files
13400	Firmware transferred to the device successfully	Covers all kind of firmware files
13500	Firmware files read/exported from the device successfully	Covers all kind of firmware files
13520	Certificates transferred to the device successfully	
13560	Exported/read archive file from the device successfully	Covers all kind of archive files
13570	Exported/read diagnosis file from the device successfully	
13580	Exported/read certificates from device successfully	Covers all kind of certificates
13900	Security logs read/exported from the device successfully	
14200	Failed to transfer configuration to the device	Covers all kind of configuration files
14220	Failed to change the configuration	Online configuration via Web interface

Table 8: Security event types in the RTU

Event id	Event name	Comment
14250	Failed to enter configuration mode	Online configuration via Web interface
14260	Failed to exit configuration mode	Online configuration via Web interface
14300	Failed to read configuration files from the device	Covers all kind of configuration files
14400	Failed to transfer firmware to the device	Covers all kind of firmware files
14500	Failed to read firmware files from the device	Covers all kind of firmware files
14520	Failed to transfer certificates to the device	
14560	Failed to read archive file from the device	Covers all kind of archive files
14570	Failed to read diagnosis file from the device	
14580	Failed to read certificates from the device	Covers all kind of certificates
14900	Failed to read security logs from the device	
23100	Password file transferred and stored in the device successfully	
23200	Password file read/exported from the device successfully	
23500	Failed to transfer password file to the device	
23600	Failed to read password file from the device	

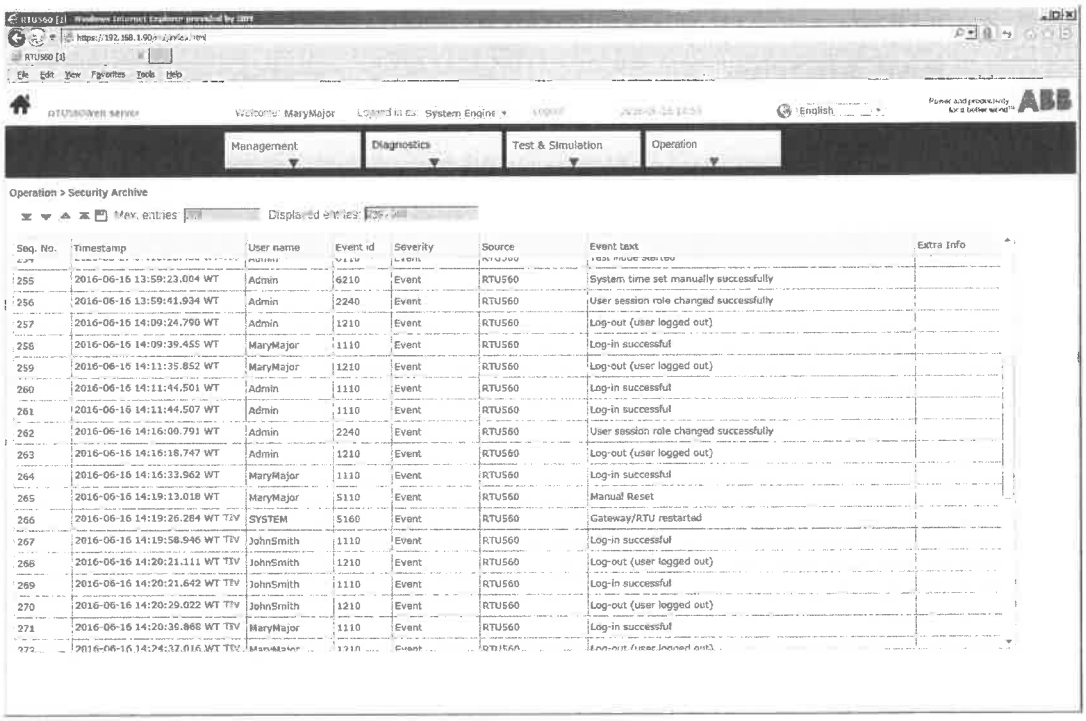
Table 8: Security event types in the RTU

4.3 View security events

To view the security event archive in the RTU500 series Web server the link "Security Archive" must be selected. This link can be found under the menu item "Operation" as shown in the figure below.

Figure 34: Web server menu security archive

One page of the security event list shows in maximum 50 events. An example of the event archive is shown in the next figure.



Seq. No.	Timestamp	User name	Event id	Severity	Source	Event text	Extra Info
255	2016-06-16 13:59:23.004 WT	Admin	6210	Event	RTU560	System time set manually successfully	
256	2016-06-16 13:59:41.934 WT	Admin	2240	Event	RTU560	User session role changed successfully	
257	2016-06-16 14:09:24.790 WT	Admin	1210	Event	RTU560	Log-out (user logged out)	
258	2016-06-16 14:09:39.455 WT	MaryMajor	1110	Event	RTU560	Log-in successful	
259	2016-06-16 14:11:35.852 WT	MaryMajor	1210	Event	RTU560	Log-out (user logged out)	
260	2016-06-16 14:11:44.501 WT	Admin	1110	Event	RTU560	Log-in successful	
261	2016-06-16 14:11:44.507 WT	Admin	1110	Event	RTU560	Log-in successful	
262	2016-06-16 14:16:00.791 WT	Admin	2240	Event	RTU560	User session role changed successfully	
263	2016-06-16 14:16:18.747 WT	Admin	1210	Event	RTU560	Log-out (user logged out)	
264	2016-06-16 14:16:33.962 WT	MaryMajor	1110	Event	RTU560	Log-in successful	
265	2016-06-16 14:19:13.018 WT	MaryMajor	5110	Event	RTU560	Manual Reset	
266	2016-06-16 14:19:26.284 WT TDV	SYSTEM	5160	Event	RTU560	Gateway/RTU restarted	
267	2016-06-16 14:19:58.946 WT TDV	JohnSmith	1110	Event	RTU560	Log-in successful	
268	2016-06-16 14:20:21.111 WT TDV	JohnSmith	1210	Event	RTU560	Log-out (user logged out)	
269	2016-06-16 14:20:21.642 WT TDV	JohnSmith	1110	Event	RTU560	Log-in successful	
270	2016-06-16 14:20:29.022 WT TDV	JohnSmith	1210	Event	RTU560	Log-out (user logged out)	
271	2016-06-16 14:20:36.868 WT TDV	MaryMajor	1110	Event	RTU560	Log-in successful	

Figure 35: Displaying security event archive

To navigate inside the list there are several buttons above the list. The buttons have the following meanings (from left to right):

- Go to end of the security event list to show the newest entries.
- To scroll one page forward in the event list (towards newer entries).
- To scroll one page backward in the event list (towards older entries).
- Go to beginning of the security event list to show the oldest entries.
- Download complete security event list in predefined CSV format.

For displaying and downloading of the security event list the following definitions apply:

- For each security event an event text is shown. The text depends on the specific event id and is in the language selected for the whole RTU500 series Web server. To change the event text, the text must be modified in the language file of the Web server (like the other texts in the Web server as well).
- All time stamps of the security events are shown in local time (local time zone) as defined for the whole RTU.
- When downloading the security event list the resulting CSV file contains the events in the same format and language as shown in the Web server display. This applies as well for the time stamps that are in local time.
- The size of the security event archive is configurable in RTUtil500. If the configured limit is reached the oldest security events in the archive are overwritten, when new events occur.

For more information about the localization support please refer to the RTU500 series Web server documentation. For detailed information about the available security event archive limits see chapter "RTUtil500 configuration".

4.4 Supervisory monitoring: security indications and alarms

To be able to monitor security events, map them to any host protocol and to make them available to the RTU internal functions PLC, logic functions, process archive and integrated HMI, it is possible to map one or more security events to indications.

Security events can be defined as input parameter of the new logic functions "Security indication" and "Security alarm". The output parameter of these functions is an indication, which can be configured and used like any other indication.

For details about the logical functions "Security event" and "Security alarm" see RTU500 series function description - part 5: SCADA functions (1KGT 150 944), chapter "Logic Functions"

4.5 External log servers

To send security events to external log servers the RTU supports up to 3 log servers per Ethernet interface on a CMU. For each log server an individual type and target IP address/ port can be configured. The following parameters are configurable within RTUtil500:

- Option to enable sending of security events to external log servers. Disabled by default.
- Protocol type of the external log server. The RTU supports the protocols Syslog UDP, Syslog TCP and ArcSight TCP.
- Target IP address of the external log server.
- Target IP port of the external log server. Each configurable type is defined with a default port that can be changed (see chapter "Ethernet ports" for the defined default ports).

In RTUtil500 the external security log servers are added at a CMU module for one or more Ethernet interfaces (Hardware tree only). The figure below shows the RTUtil500 dialog to add an external security log server at the first Ethernet interface.

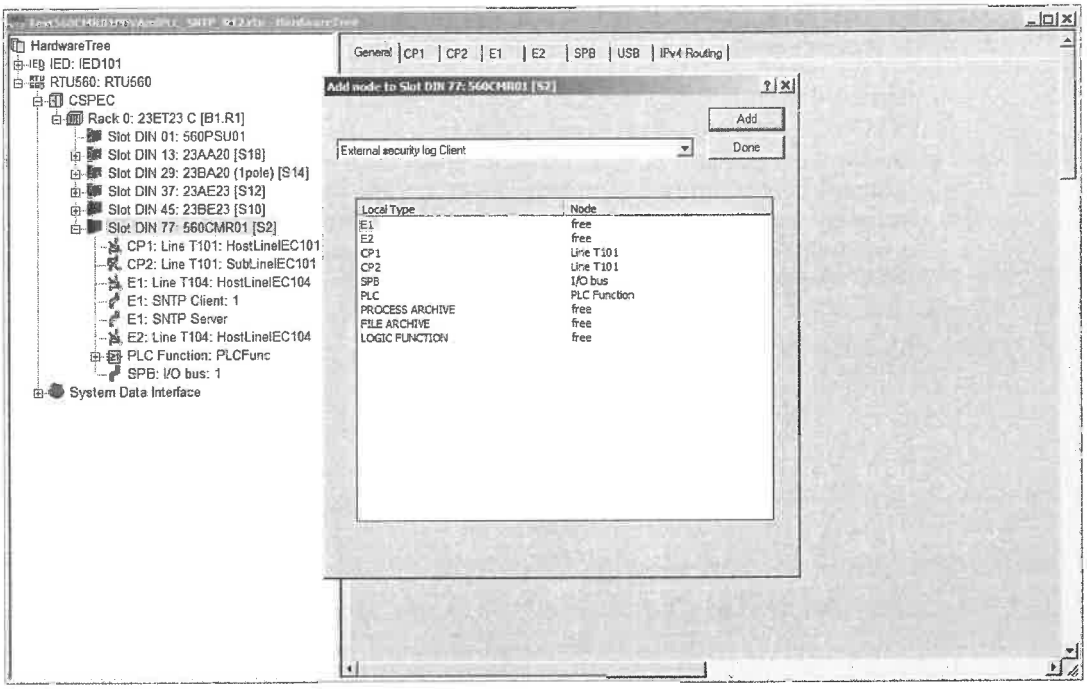


Figure 36: RTUtil500 add external security log server

In case the CMU supports more than one Ethernet interface, the external log servers can be added to all interfaces or to each Ethernet interface individually. To configure the parameters of the external log servers, the log server has to be selected in the hardware tree (below the CMU) and the tab "External Security Log Server" has to be opened. The next figure shows these configuration parameters.

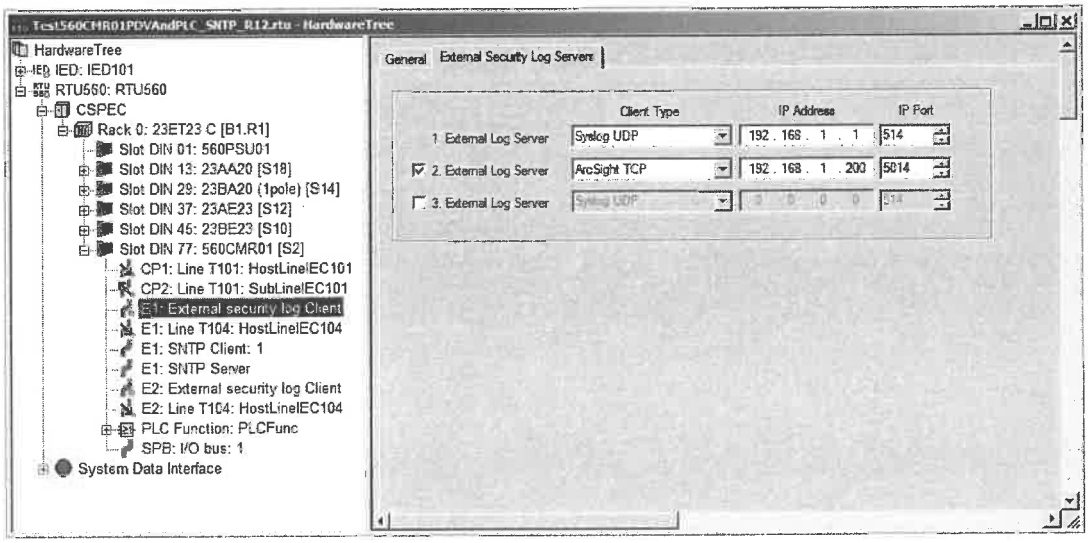


Figure 37: RTUtil500 external log server parameter

In this tab the described parameters for external security log servers are configured. The consistency check of RTUtil500 displays a warning if an external log server is enabled but no target IP address or IP port are configured.

The security events are sent to the external log servers at the moment the event occurs. The security events are sent in the format defined for the supported protocols. Please refer to the protocol description of Syslog and ArcSight for detailed information about the event format.

If the external log server is not available at the moment an event occurs the handling in the RTU depends on the type of log server. The following handling is supported:

- Syslog UDP: Due to the unconfirmed UDP protocol the event is send on the network but lost in case the log server is not available.
- Syslog TCP, ArcSight TCP: An occurred event is stored in a small FIFO queue (maximum 10 entries) before sending to the log server. In case the log server is not available the event remains stored in the FIFO queue and the RTU tries to send the event to the log server in cyclic intervals. If the FIFO queue is full new events are lost. After a restart of the RTU the FIFO queue is erased and not sent events are lost.

5 Secure Web server access

For secure access, the RTU500 series Web server supports Hypertext Transfer Protocol Secure (HTTPS). HTTPS is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server. Detailed information about HTTPS could be found in RFC2818 "HTTP Over TLS".

For the identification the RTU500 series Web server uses as default self-signed public key certificates not issued by a certification authority (CA). The default self-signed certificates are created at startup depending on the configuration. In addition the RTU500 series Web server supports the upload of external generated HTTPs certificates. This allows to use trusted certificates issued by a certification authority (CA).

Client authentication with user certificates is not supported by the RTU500 series. The authentication of the user is ensured by a user name and a password.

ADVICE
For security reasons, the web client has to be closed after each working session. This prevents the usage of supplied user names and passwords by unauthorized persons.

The following chapters describe configuration, access and certificate handling for the secured RTU500 series Web server.

5.1 RTUtil500 configuration

The configuration parameters for the Web server access are defined for each CMU respectively Ethernet interface within an RTU. The following parameters are configurable within RTUtil500:

- Option to disable the Web server on selected Ethernet interfaces. This is possible in single and multiple CMU systems. The Web server must be enabled on at least one Ethernet interface to be able to access the RTU at all. The Web server is enabled on all Ethernet interfaces by default.
- Option to secure the Web server access with HTTPS. This option can be selected on each CMU. The HTTPS option is enabled by default
- Define the authentication type for the secure Web server. Possible are the default self-signed certificate or an uploaded external certificate stored in the certificate store of the CMU.
- Set an entry in the certificate store of the CMU to upload external HTTPS certificates for the Web server authentication.

In RTUtil500 the option to disable the Web server is placed at the CMU in the configuration tab of the Ethernet interface, e.g." E1" (Hardware tree only). The figure below shows the option in the RTUtil500 user interface. The Web server is disabled by deselecting the checkbox "Enable Web server".

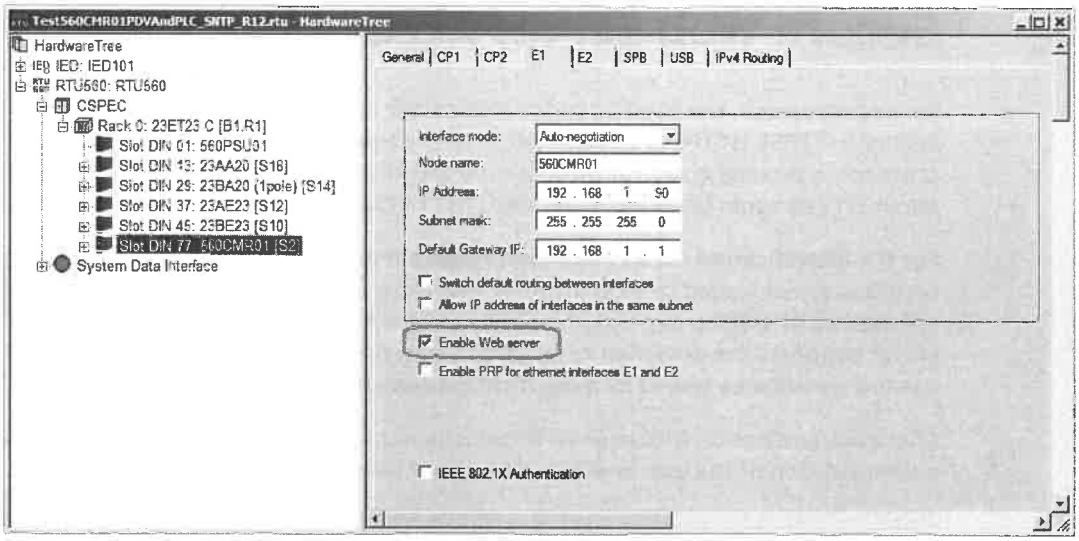


Figure 38: RTUtil500 Ethernet interface Web server parameter

As shown in the next figure, the configuration parameters related to the secure Web server are located in the "General" tap at a CMU module (Hardware tree only). To secure the RTU500 series Web server with a self-signed certificate follows these steps:

1 Select the checkbox "Secure HTTPS Web server".
2 Select the option "Self-created and self-signed certificate" in the drop-down menu "Web-server authentication" (shall be pre-selected).

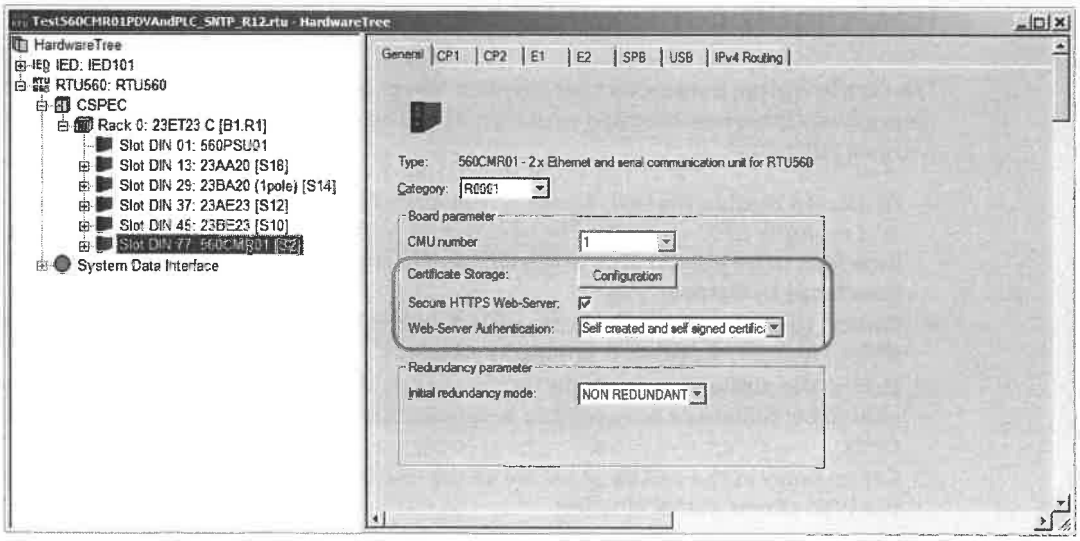


Figure 39: RTUtil500 secure Web server parameter

For the usage of an external HTTPS certificate, the certificate store has to be configured at first. That means an entry has to be added to the certificate store representing the certificate used for the Web server authentication.

The certificate store configuration opens by pressing the button "Configuration" shown in the figure above (near the text "Certificate Storage"). When selected a dialog appears with several entries for certificates. Each entry represents a certificate that shall be transferred to the CMU. To add a certificate, select the check box at the entry number and give the entry a descriptive name. An example of the certificate store configuration is shown in the figure below.

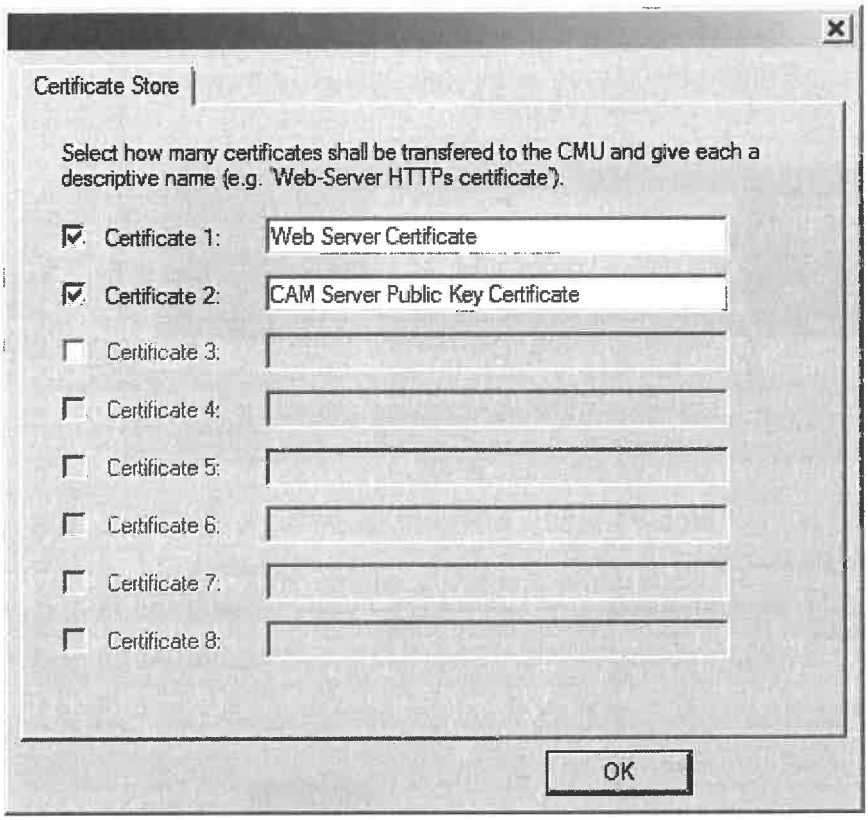


Figure 40: RTUtil500 certificate store

Together with the certificate store the steps to secure the RTU500 series Web server with an external certificate are:

1 Configure an entry in the certificate store representing the external certificate to upload. Give the entry a descriptive name like "Web server certificate".
2 Select the checkbox "Secure HTTPS Web server".
3 Select in the drop-down menu "Web-server authentication" the certificate from the store. Here the name given in the first step is selected.
4 Upload the external HTTPS certificate via the RTU500 series Web server.

Further information about the upload of external HTTPS certificates can be found in the chapters "External certificate" and "Certificate management".

5.2 Web server user authentication

After a successful connection with a Web browser to the RTU500 series Web server, the server requests a user name and password for log-in. The log-in dialog presented by the Web browser depends on the configuration of the RTU. With the local user account management (LAM) a standard log-in dialog, generated by the Web browser itself, appears. Examples for this kind of log-in dialog are shown in the next figure. The Examples are from the Microsoft Internet Explorer and the Google Chrome Browser.

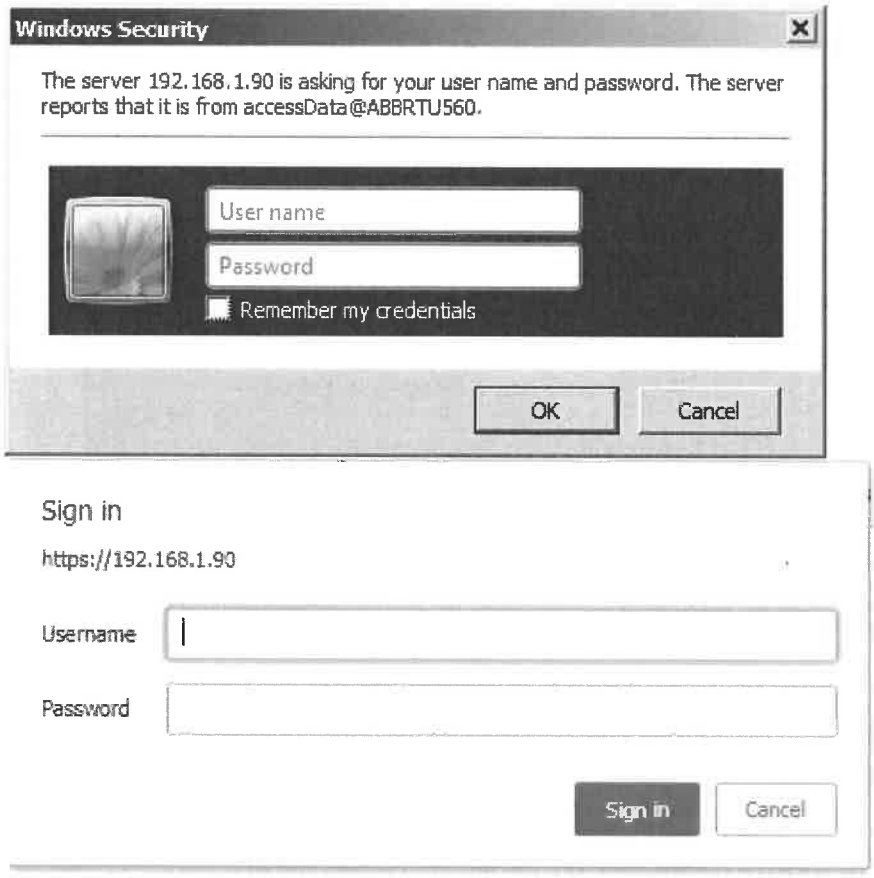


Figure 41: LAM log-in dialog examples

With the central user account management (CAM) a common log-in dialog, generated by the Web server, is shown (see figure below). Additional to the input fields for user name and password the dialog contains an information whether the CAM server is available or not. This information named protection space can have the following values:

- CAM Server
  CAM server connection is online. Login via CAM server is required.
- LAM Backup
  CAM server connection is offline and LAM is configured as backup. Login is possible via LAM.
- Not available
  CAM server connection is offline and LAM is not configured as backup. No login is possible.

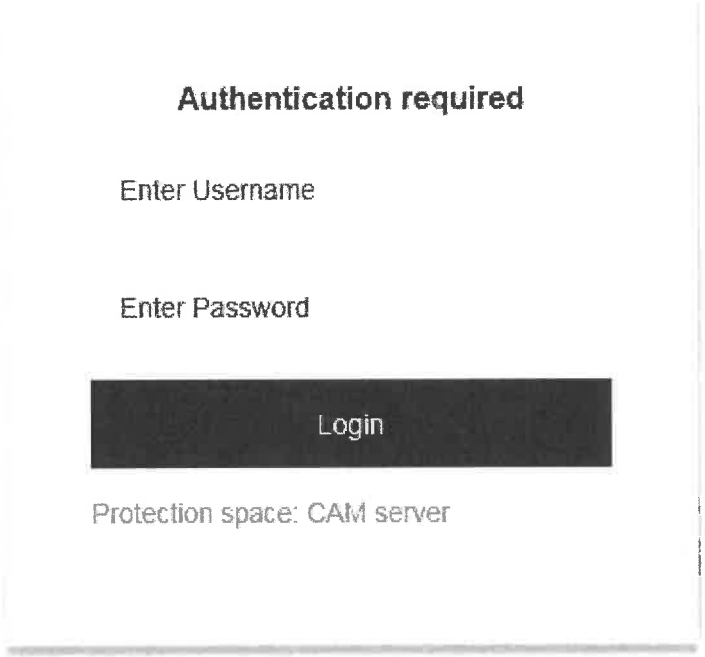


Figure 42: CAM log-in dialog

To avoid unsecure configuration in connection with the central user account management (CAM) the following advice shall be considered.

ADVICE
In a CAM configuration the user credentials are transmitted as plain text from the Web browser to the RTU500 series. Therefore the secure Web server access via HTTPS shall be enabled for the RTU500 series if a CAM client is used. This applies for all CMU modules in a multi CMU setup.

5.3 HTTPS Web server access

To access the RTU500 series Web server via HTTPS the URL given in the Web client must begin with "https://" followed by the IP address of the RTU. The following figure shows an example.

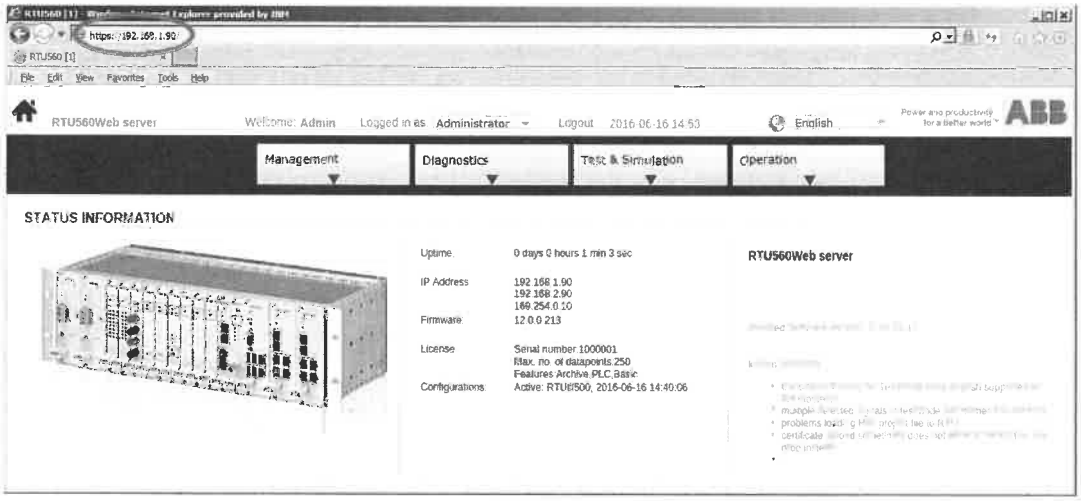


Figure 43: HTTPS access to an RTU Web server

The default Web server certificates used by the RTU500 series are self-signed and not issued by a certification authority (CA). As result an actual web client shows a warning messages concerning the missing CA, if the Web server is accessed with HTTPS. To avoid this warning message a trusted external certificate must be configured and uploaded to the RTU500 series.

If the Web server is configured for HTTPS a standard access is not possible anymore. In case of a standard access the Web server redirects the access to the secure pages of the RTU500 series Web server.

If the Web server is not configured for HTTPS, a secure access is possible as well. There are no restrictions in this case besides the possible warning message from the self-signed certificate.

See chapter "RTUtil500 configuration" for configuration and chapter "External certificate" for upload of external certificates.

5.4 Certificate handling

For encryption and secure identification HTTPS uses public key certificates that bind together a public key with an identity (information such as the name of an organization, their address and so on). The certificate is used to verify that a public key belongs to an identity. In case of HTTPS the Web server presents the certificate to the web client giving the client the public key and the identity of the server.

The public key is one part of an asymmetric key algorithm, where the key used to encrypt a message is not the same as the key to decrypt it. Messages encrypted with the public key can only be decrypted with the other part of the algorithm the private key. Public and private key are related mathematically and represents a cryptographic key pair. The private key must be kept secret, whilst the public key may be widely distributed.

This requires for the RTU a public/private key pair and a corresponding public key certificate. There are two possibilities for this purpose. First the self-signed certificates generated by the RTU500 series firmware can be used or a trusted, extern generated certificate can be uploaded to the RTU. When uploading, a certificate must be available for each CMU because the Web server can be accessed on any CMU. Further information about the self-signed and extern generated certificates can be found in the following two chapters.

5.4.1 Self-signed certificate

In the default setup the RTU500 series Web server uses self-generated and self-signed public key certificates for encryption and secure identification. As explained above the certificate consists of a public/private key pair and an identity information. The key pair and the certificate are generated by the RTU firmware and stored in the internal flash of the CMU (not on the memory card).

The following procedure is executed the first time the RTU firmware starts:

1 Generate an RSA public/private key pair depending on random conditions.
2 Generate a certificate with predefined identity information (see below for more information).
3 Bind together certificate and public key with a digital signature (self-sign certificate).
4 Encrypt the public/private key pair with a symmetric key provided by the RTU firmware.
5 Store the encrypted key pair and the public key certificate in the internal flash of the CMU.

The usage of the private/public key pair and the certificate for the Web server communication are explained in the following figure.

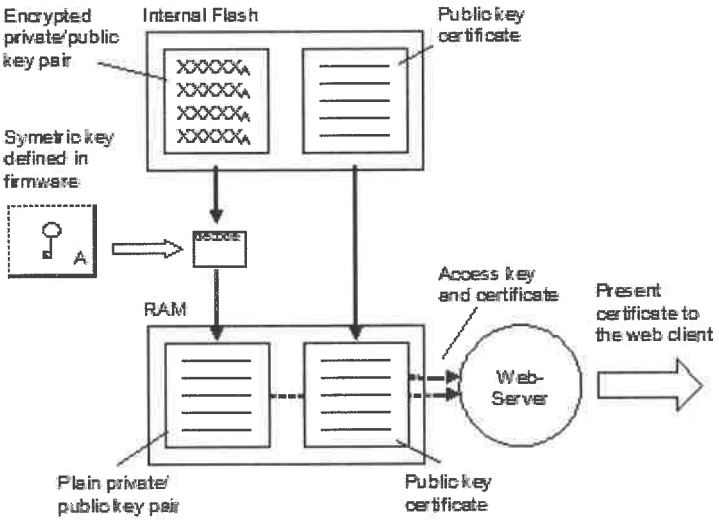


Figure 44: Usage of key pair and certificate within an RTU500 CMU

As described the internal flash of the CMU contains the encrypted private/public key pair and the public key certificate. The key pair is read from the flash, decoded with a symmetric key defined in the firmware and stored in the RAM of the CMU. The certificate is read as it is from the flash memory and stored in the RAM as well.

The Web server accesses the public key certificate (stored in RAM) and presents it to web client during the HTTPS protocol. The private key is used by the Web server to decrypt messages, encrypted by the web client with the public key. For further information about the HTTPS protocol see RFC2818 "HTTP Over TLS".

The certificate contains HTTPS protocol specific information like the public key and identity information. The identity information are set as follows.

- The identity information like country, locality and organization name are predefined to the ABB AG, Mannheim, Germany. These cannot be changed.

- The common name of the identity is set to the configured IP address of the CMU Ethernet interface E1. The common name represents the host name (server name) the web client uses to access the Web server. In case the configuration of the IP address changes a new certificate is generated and stored in the internal flash (overwrites the existing one).
- In subject alternative name the IP address of the Ethernet interface E1 and the USB interface are defined. This allows the secure HTTPS access via USB as well.
- The serial number of the certificate is set to 1 for the first created certificate and increased every time a new certificate is generated due to a configuration change.
- The expiration date of the certificate is set the 1. January 2070.

5.4.2 External certificate

The RTU500 series supports the usage of external generated and signed public-key certificates for the encryption and secure identification of the Web server. These certificates can be uploaded to the RTU500 series via the Web server. When creating an end-entity certificate for the RTU500 series Web server the following issues shall be considered:

- The generated end-entity server certificate shall be signed and issued by a trusted root or intermediate certificate. This avoids any warning messages in the Web client when accessing the RTU500 series Web server via HTTPS.
- For a correct end-entity Web server certificate the attribute "keyUsage" must contain the encryption values "keyEncipherment" and "dataEncipherment", at least. And the attribute "extendedKeyUsage" must contain the server authentication value "serverAuth".
- The common name of the certificate identity must not be set to an IP address used in the RTU. It is sufficient to set the attribute "IP Address" in the subject alternative name to a used IP address. Depending on the policies in your organization setting the attribute "DNS Name" might be necessary as well.
- To use the same certificate for several CMU's or RTU's a list of IP addresses and DNS names can be defined in the subject alternative name.
- The generated certificate must contain the public/private key pair of the end-entity certificate. The whole certificate chain, including root and intermediate certificates can be included but this is not required.
- For uploading the generated certificate must be stored in PKCS#12 format with the file ending ".p12".

After uploading the external generated certificate, the certificate is stored as file on the memory card of the CMU. In the Web server communication this certificate is used as explained in the next figure.

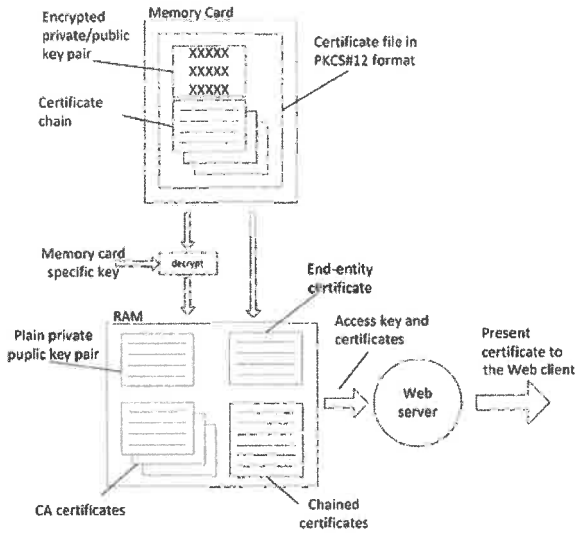


Figure 45: Usage of uploaded certificate within an RTU500 CMU

At startup the PKCS#12 certificate file stored on the memory card is parsed and first the encrypted private/public key pair is decoded with a memory card specific key. The resulting plain private/public key pair is stored in the RAM for the Web server. Then the end-entity certificate and the CA certificates are extracted from the PKCS#12 file and stored in the RAM as well. At last all CA certificates are combined to a certificate chain that is presented to the web client.

The Web server accesses the certificates (stored in RAM) and presents it to web client during the HTTPS protocol. The private key is used by the Web server to decrypt messages, encrypted by the web client with the public key. For further information about the HTTPS protocol see RFC2818 “HTTP Over TLS”.

The upload of an external generated certificate is done via the RTU500 series Web server. For detailed information about the upload process see chapter "Certificate management". When the upload is finished the RTU500 series has to be restarted to activate the Web server certificate. And it may be necessary to restart the Web client as well, to recognize the new certificate in the client

6 Certificate management

For several security functionalities in the RTU500 series external generated certificates are required. Examples of these functionalities are the central user account management (see chapter "Central user account management") and the secure Web server (see chapter "Secure Web server access"). In either case the external certificates must be uploaded via the web interface of the RTU500 series. The following chapter describes the process to upload these certificates.

6.1 Certificate upload

In the Web server menu, the link "Certificate Management" is the entry point for the certificate upload. This link can be found under the menu item "Management" as shown in the figure below. Due to the sensible information in the certificate upload the following notice has to be considered.

ADVICE

The web pages of this functionality require secure HTTPS access. It is not possible to open the web pages with standard HTTP access.

Figure 46: Web server menu certificate management

In the certificate management, the certificates for different functionalities can be uploaded to the RTU500 series. Generally there are two types of certificates with the following characteristics:

- Public Key certificates
  These certificates contain the public key of a server certificate. The certificate type is used for client activities in the RTU500 series like the central user account management (CAM). As the certificates contain public information only, no password is required for the upload. The public key certificates must in PKCS#7 format and the file extension must be "*.p7b".
- Private Key certificates
  These certificates contain end-entity certificate with public/private key pair and possibly the whole certificate chain. The certificates are used for server activities in the RTU500 series like the Web server. For the upload the passphrase of the private key is required. The private key certificates must in PKCS#12 format and the file extension must be "*.p12".

The user interface for the certificate upload is separated in two areas. The upper area contains the certificates actually uploaded to the RTU500 series and the lower area controls the upload. The following figure shows an example with two certificates to upload. One

public key certificate for CAM and a private key certificate for the Web server. As there is no trusted, certificate for the Web server uploaded in the example, a certificate error is shown. This error is dissolved after the upload of the Web server certificate (see last figure in this chapter).

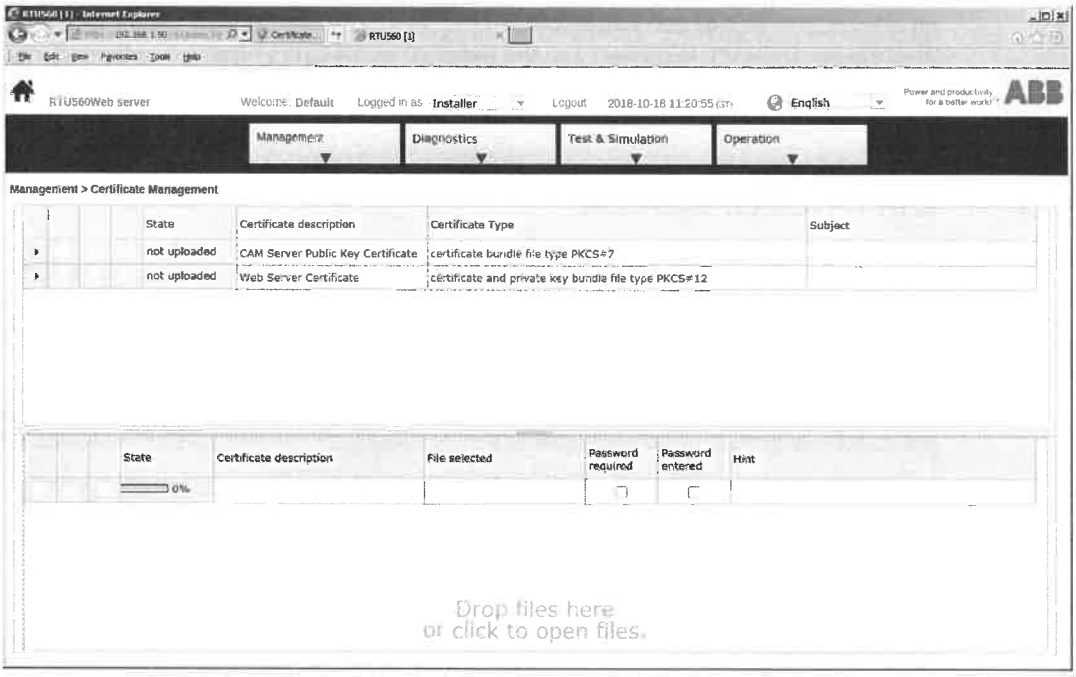


Figure 47: Certificate management user interface

To upload a certificate the following steps has to be executed in the lower area of the user interface:

1 Select the description of the certificate to upload in the column "Certificate description". In the selection all in RTUtil500 configured entries of the certificate store appear. The selection text is the descriptive name set in RTUtil500 as explained in the chapter about the RTUtil500 configuration. The type of certificate to upload is written in the column "Certificate Type" of the upper area.
2 Select a certificate file by dropping the file on the lower area or by using the file open dialog that appears when clicked with the mouse. Depending on the certificate type, the file must be in PKCS#7 or PKCS#12 format.
3 If a private key certificate is uploaded the password respectively passphrase of the private key is required. To enter the passphrase select the lock symbol on the left side. When pressed a dialog appears to enter the passphrase. The passphrase is used to decrypt the private key of the certificate after the upload. For storing on the memory card the private key is re-encrypted with a memory card specific key. The entered passphrase is not stored on the RTU500 series. For public key certificates no passphrase is required.

When all steps are finished the certificate can be uploaded by pressing the upload button (see figure below). The upload button appears not before all required information are set.

Figure 48: Start certificate upload

Depending on the activity that uses the uploaded certificate, it may be necessary to restart the RTU500 series for activation of the certificate. Please refer to the specific activity documentation to find the information whether a restart is required or not. In the example shown here the Web server certificate requires a restart but the CAM certificate not.

After a successful upload and activation the certificate management looks like shown in the next figure. The upper area contains now the information about the uploaded certificates and the certificate error due to the missing trusted Web server certificate is not shown anymore.

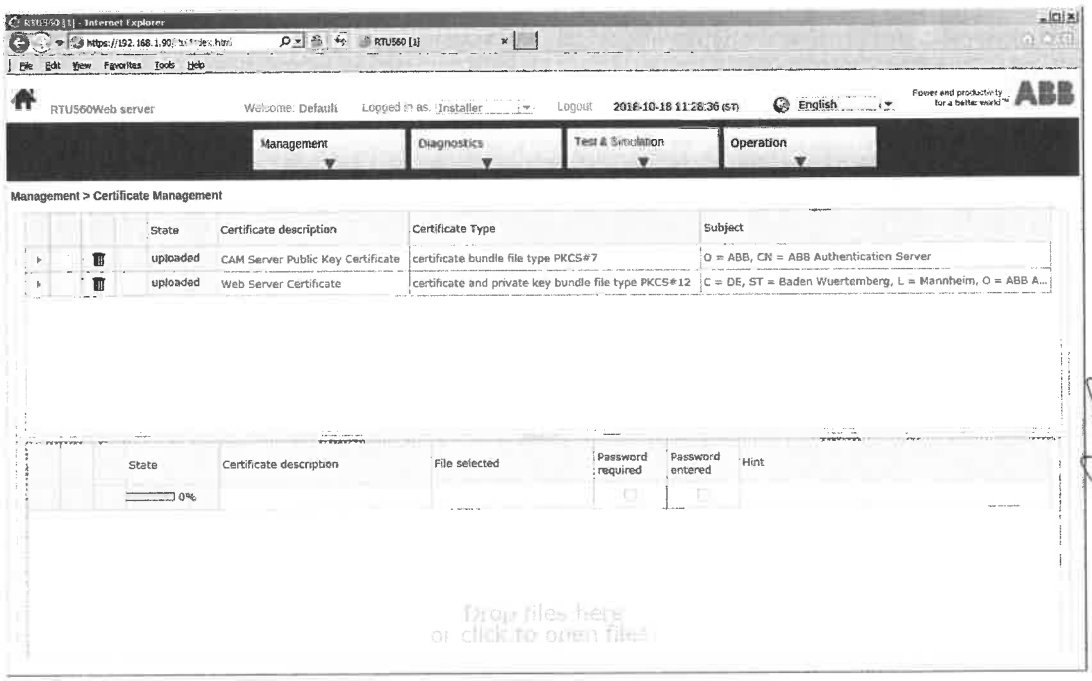


Figure 49: Certificate upload successfully finished

7 IEEE 802.1X Port-based Network Access Control

7.1 Technology Overview

IEEE 802.1X is a security standard for port-based network access control that secures wired networks against unauthorized access by requiring authentication with a central server before network access and data transmission are allowed.

A port is a point of attachment to a network. IEEE 802.1X provides port-based network access control that allows network access decisions made at the port, on a per-port basis using the EAPOL (Extensible Authentication Protocol Over LAN). For a wired network, a port could be where the MAC (Media Access Control) physically attaches to the network, such as a switch port.

The purpose of IEEE 802.1X is authentication of Ethernet network equipment. Equipment that is not authenticated will not even receive link. Only equipment that is authenticated should get network access when connected to an Ethernet switch.

There is a client implementation of IEEE 802.1X in RTU500. That means RTU500 provides IEEE 802.1X supplicant role on Ethernet interface E1 and if present on E2 of a CMU module. The RTU500 sends authentication information in the form of a X.509 certificate or username/ password to the authenticator and requests access to the network.

The supplicant uses EAPOL that uses data link layer (Layer 2) for communication with the authenticator. The authenticator is the switch in the substation that controls access to the network. The authenticator forwards authentication requests from the supplicant to the authentication server. When the authenticator receives an EAPOL packet from the supplicant it packets them in a radius format and then forwards them to the authentication server. The authentication server checks if the supplicant should be allowed network access and reports this back to the authenticator.

Before the RTU500 has allowed access the authenticator puts the access port in unauthorized mode. In this mode only EAPOL traffic is allowed on the port. As soon as the RTU500 has allowed access the port changes to authorized mode and other traffic is allowed.

7.2 EAP (Extensible Authentication Protocol)

IEEE 802.1X uses EAP to define how messages used for authentication are sent between devices. EAP is using layer 2 (data link) and can therefore send information without valid IP address.

RTU500 supports the following EAP types:

- EAP-TLS (X.509 certificate-based authentication)
- EAP-PEAPv0 with EAP-MSCHAPv2

EAP-TLS (Transport Layer Security) is an IETF (Internet Engineering Task Force) open standard that uses the TLS protocol, and is well-supported among vendors. RTU500 EAP complies with the IETF RFC 5216: The EAP-TLS Authentication Protocol. EAP-TLS is an EAP type that make use of TLS to perform mutual authentication between the client and server. TLS exploits the properties of asymmetric cryptography by means of certificate exchange between peers. EAP-TLS requires that both server-side and client-side certificates are

deployed. EAP-TLS uses PKI (Public Key Infrastructure) to secure communication to a RADIUS (Remote Authentication Dial-In User Service) authentication server.

EAP-PEAPv0 (Protected EAP) uses server-side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server. The ensuing exchange of authentication information to authenticate the client is then encrypted and user credentials are safe from eavesdropping. EAP-MSCHAPv2 (Microsoft-Challenge-Handshake Authentication Protocol version 2) is tunneled through TLS as inner authentication type for EAP-PEAPv0.

7.3 RTUtil500 configuration

The configuration parameters for IEEE 802.1X Port-based Network Access Control are defined for each Ethernet interface within an RTU.

A checkbox "IEEE 802.1X Authentication" is available on Ethernet interface E1 and if present E2 tab of a CMU module to enable the supplicant functionality.

Parameter name	Default	Parameter location
IEEE 802.1X Authentication	disabled	CMU - Network Interfaces
If the option is checked, IEEE 802.1X Port-based Network Access Control will be enabled.		

The following parameters are configured in a separate dialog accessible via "Configuration" button.

Parameter name	Default	Parameter location
EAP Identity		CMU - Network Interfaces
The identity sent in response messages to the authenticator.		
EAP-TLS	disabled	CMU - Network Interfaces
If the option is checked, Extensible Authentication Protocol type Transport Layer Security (TLS) will be enabled.		
Certificate-based authentication		CMU - Network Interfaces
Select a certificate used for IEEE 802.1X authentication. List items depend on certificate store configuration, that means prior to that list selection set an entry with descriptive text in the certificate store of the CMU module to upload external certificates for the IEEE 802.1X authentication.		
EAP-PEAPv0	disabled	CMU - Network Interfaces
If the option is checked, Extensible Authentication Protocol type Protected EAP (PEAPv0) will be enabled.		
EAP-MSCHAPv2	disabled	CMU - Network Interfaces
If the option is checked, Extensible Authentication Protocol type Microsoft-Challenge-Handshake Authentication Protocol version 2 (MSCHAPv2) will be enabled.		
MSCHAPv2 User ID		CMU - Network Interfaces
The user-id used in MSCHAPv2 handshakes.		
MSCHAPv2 Password		CMU - Network Interfaces
The password used in MSCHAPv2 handshakes.		

7.4 Certificate upload via the RTU500 Web server

A digital certificate is used to prove that someone is who they say they are. In an 802.1X negotiation, the authentication server uses certificates to prove its identity to the supplicant.

The certificates used by the authentication server are called server certificates. The certificates used by the supplicant are called client certificates. Server certificates are required for EAP-TLS and EAP-PEAPv0. EAP-TLS requires that the RTU500 prove its identity with a client certificate as well.

EAP-TLS requires an uploaded external certificate stored in the certificate store of the CMU module. The web pages for certificate configuration require secure HTTPS Web server access. It is not possible to open the web pages with standard HTTP access. For uploading the generated certificate must be stored in PKCS#12 format.

The upload of an external generated certificate is done via the RTU500 Web server. In the Web server menu the link 'Certificate Management' is the entry point for the certificate upload. This link can be found under the menu item 'Management'.

To upload a certificate the following steps have to be executed:

- Select the description of the certificate to upload in the column 'Certificate description'. In the selection all in RTUtil500 configured entries of the certificate store appear. The selection text is the descriptive name set in RTUtil500.
- Select a certificate file.
- Enter the private key password by pressing the lock symbol.

When all steps are finished the certificate can be uploaded by pressing the button 'Send file to device'. This button appears not before all required information are set. Further information about the upload of external certificates can be found in User Manual RTU500 series Web Server Release 12 (1KGT 150 924).

8 System hardening

ABB strives to improve the security and robustness of its products by performing security testing and hardening.RTU500 series has been systematically hardened, e.g. unused services have been removed and unused ports closed. Furthermore RTU500 series has been thoroughly tested at ABB's dedicated, independent security test center using state-of-the-art commercial and open-source security testing tools. Security testing and hardening are integrated parts of the development process.

9 Patch management

9.1 General information

This chapter describes the patch management for the RTU500 series and how to keep the system up to date.

Three categories of updates are available for the RTU500 series:

- Patches (cyber security updates)
- Bug fixes (available for the latest minor release)
- Minor/Major releases (new functions)

Most of the cyber security issues can be solved by patches (e.g. OS patches, fixes in protocols).

Partly minor/major release change is required (e.g. new encryption, new OS versions, new cyber security functions).

Firmware updates and patches are available via the local service partner.

9.2 Release policy

The Release policy of the RTU500 series is as follows:

- Patches based on security vulnerability (e.g. Poodle) on request.
- Bug fix releases on request (typically every 6-10 weeks).
- Project specific developments are tested as beta version and will be released with the next minor or major release.
- Two minor/major releases per year with functional improvements.

9.3 Update policy

The Update policy of the RTU500 series is as follows:

Patch: Updates in cyber security functions

- No changes in RTU configuration
- Test recommendation in the release note

Bug fix: Error corrections

- No changes in RTU configuration
- Functional test of corrected function is recommended

Minor release:

- New RTU and new cyber security functions
- Update of RTU configurations and parameter changes
- Functional test of updated/new function is recommended

Major release:

- New RTU and new cyber security functions
- Migration of RTU configurations and parameter changes
- Migration guide is available
- Functional test of updated/new function is recommended

9.4 Recommendation by ABB

We recommend to implement cyber security patches as soon as possible.

Information are available at:

- ABB Inside: Internal announced findings and solutions
- www.abb.com/remote-terminal-units: Official information for end customers

Bug fixes have to be implemented only if it is relevant for the running system.

Annual minor/major release updates are recommended:

- At least minor release update
- Major release updates shall be considered

9.5 Patch installation

For patch installation please consider following points:

- Login to the RTU with required user rights.
- Download the new firmware version via web server.
- Configuration file stays unchanged.
- Restart the RTU.
- You can find logged installation procedure in the security log.

10 Compliance Statement

This chapter contains a compliance statement of the RTU security functionality against IEEE 1686 standard. Considered is the chapter "IED Cyber Security Features".

10.1 Electronic Access Control

IEEE chapter no	IEEE chapter name	Compliance
5.1	Electronic Access Control	Comply
5.1.1	IED Access Control Overview	Comply
5.1.2	Password Defeat Mechanisms	Comply
5.1.3	Number of Individual Users	Comply
5.1.4	Password construction	Comply
5.1.5	IED access control	Comply
5.1.5.1	Authorization Levels by Password	Comply
5.1.5.2	Authorization using role-based access control (RBAC)	Comply
5.1.6	IED main security functions	Comply
5.1.6 a)	View Data	Comply
5.1.6 b)	View Configuration Settings	Comply
5.1.6 c)	Force Values	Comply
5.1.6 d)	Configuration Change	Comply
5.1.6 e)	Firmware Change	Comply
5.1.6 f)	ID/Password Management	Comply
5.1.6 g)	Audit trail	Comply
5.1.7	Password Display	Comply
5.1.8	Access Timeout	Comply[1]

Table 9: IEEE 1686 compliance "Electronic access"

1 The access time-out is retriggered with every user action. The time-out is configurable in a range between 1 minute and 24 hours. The time-out can be disabled by setting to 0.

10.2 Audit Trail

IEEE chapter no	IEEE chapter name	Compliance
5.2	Audit Trail	Comply
5.2.2	Storage Capability	Comply[1]
5.2.3	Storage Record	Comply
5.2.3 a)	Event Record Number	Comply
5.2.3 b)	Time and Date	Comply
5.2.3 c)	User Identification	Comply
5.2.3 d)	Event Type	Comply
5.2.4	Audit Trail Event Types	Comply
5.2.4 a)	Login	Comply

Table 10: IEEE 1686 compliance "Audit trail"

IEEE chapter no	IEEE chapter name	Compliance
5.2.4 b)	Manual Logout	Comply
5.2.4 c)	Timed Logout	Comply
5.2.4 d)	Value Forcing	Comply[2]
5.2.4 e)	Configuration Access	Comply
5.2.4 f)	Configuration Change	Comply
5.2.4 g)	Firmware Change	Comply
5.2.4 h)	ID/Password Creation and Modification	Comply
5.2.4 i)	ID/Password Deletion	Comply
5.2.4 j)	Audit-Log Access	Comply
5.2.4 k)	Time/Date Change	Comply[3]
5.2.4 l)	Alarm Incident	Exception[4]

Table 10: IEEE 1686 compliance "Audit trail"

1 The event log with 2048 events is available. Removing the storage media will halt the device. After reinserting of the storage media, the device must be rebooted but will then function properly unless the storage media was damaged.
2 Comply if the PLC online debug mode is disabled during normal operation (requires administrator permission). PLC online debug mode is disabled by default.
3 Comply if the test mode is disabled during normal operation. Test mode is disabled by default.
4 Not supported.

10.3 Supervisory Monitoring and Control

IEEE chapter no	IEEE chapter name	Compliance
5.3	Supervisory Monitoring and Control	Comply[1]
5.3.1	Overview of Supervisory Monitoring and Control	Comply[1]
5.3.2	Events	Comply[1]
5.3.3	Alarms	Exception[2]
5.3.3 a)	Unsuccessful Log In Attempt	Exception[4]
5.3.3 b)	Reboot	Comply
5.3.3 c)	Attempted Use of Unauthorized Configuration Software	Comply[5]
5.3.3 d)	Invalid configuration or firmware download	Exception[6]
5.3.3 e)	Unauthorized configuration or firmware file	Exception[6]
5.3.3 f)	Time signal out of tolerance	Comply
5.3.3 g)	Invalid field hardware changes	Comply
5.3.4	Alarm Point Change Detect	Comply
5.3.5	Event and Alarm Grouping	Exception[3]
5.3.6	Supervisory Permissive Control	Exception[3]

Table 11: IEEE 1686 compliance "Supervisory monitoring and control"

1 Audit trail events (security events) can be monitored at supervision and control systems with a Web client.
2 Available only for monitoring and control events like control outputs, status changes, measured values and integrated totals.

3 Not supported.
4 An unsuccessful log in attempt is detected and logged every time a wrong user credential is given.
5 All configuration and firmware changes are handled in the RTU Web server with authentication control. The PLC online debug connection is also controlled by the Web server (access deactivated by default).
6 The download of configuration and firmware is protected by user authentication, but the configuration or firmware file itself is not checked for validity and authentication.

10.4 Cyber Security Features

IEEE chapter no	IEEE chapter name	Compliance
5.4	IED cyber security features	Comply
5.4.1	IED functionality compromise	Comply
5.4.2	Specific crytographic features	Comply
5.4.2 a)	Webserver functionality	Comply
5.4.2 b)	File transfer functionality	Comply[1]
5.4.2 c)	Text-oriented terminal connections	Not applicable[2]
5.4.2 d)	Full Access	Comply
5.4.2 e)	Network time synchronization	Comply
5.4.2 f)	Secure tunnel functionality	Comply
5.4.3	Cryptographic techniques	Acknowledge
5.4.4	Encrypting serial communications	Exception[3]
5.4.5	Protocol-specific security features	Exception[4]

Table 12: IEEE 1686 compliance "Cyber security features"

1 The file transfer functionality in the RTU is implemented with Hypertext Transfer Protocol Secure (HTTPS) equal secure as Secure File-Transfer Protocol (SFTP).
2 The RTU doesn't provide any text oriented terminal connection.
3 Not supported.
4 The RTU supports IEC 62351-3 transport layer security for IEC 60870-5-104 and IEC 62351-5 secure authentication for DNP3 LAN/WAN.

10.5 Configuration Software

IEEE chapter no	IEEE chapter name	Compliance
5.5	Configuration Software	Acknowledge
5.5.1	Authentication	Comply[1]
5.5.2	Digital signature	Exception[3]
5.5.3	ID/Password Control	Not applicable[2]
5.5.4	ID/Password Controlled Features	Not applicable[2]
5.5.4.1	View Configuration Data	Not applicable[2]
5.5.4.2	Change Configuration Data	Not applicable[2]
5.5.4.2 a)	Full Access	Not applicable[2]
5.5.4.2 b)	Change tracking	Not applicable[2]
5.5.4.2 c)	Use monitoring	Not applicable[2]

Table 13: IEEE 1686 compliance "Configuration software"

IEEE chapter no	IEEE chapter name	Compliance
5.5.4.2 d)	Download to IED	Not applicable[2]

Table 13: IEEE 1686 compliance "Configuration software"

1 All configuration and firmware changes are handled in the RTU Web server with authentication control. The exception is the PLC online debug connection which is controlled by the Web server as well.
2 Not required for RTUtil500 because every access is handled via RTU Web server.
3 Not supported.

10.6 Communications Port Access

IEEE chapter no	IEEE chapter name	Compliance
5.6	Communications Port Access	Comply

Table 14: IEEE 1686 compliance "Communications port access"

10.7 Firmware Quality Control

IEEE chapter no	IEEE chapter name	Compliance
5.7	Firmware Quality Control	Exception[1]

Table 15: IEEE 1686 compliance "Firmware quality control"

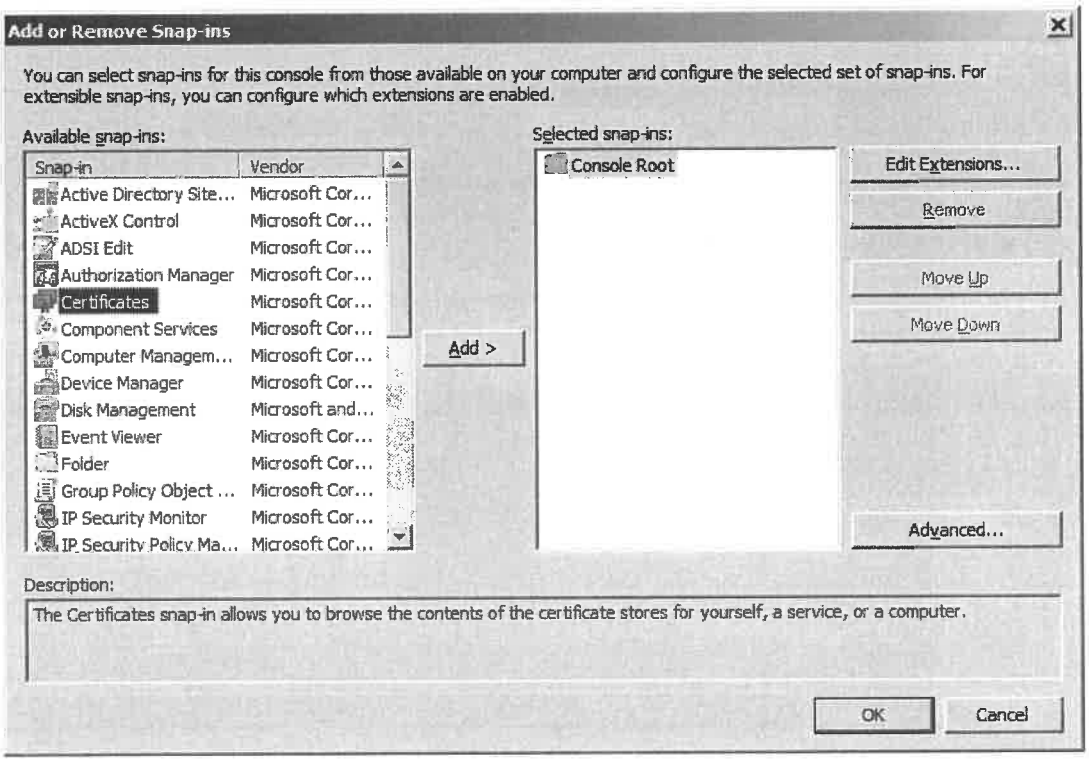
1 Quality control is handled according to ISO9001

11 Appendix A

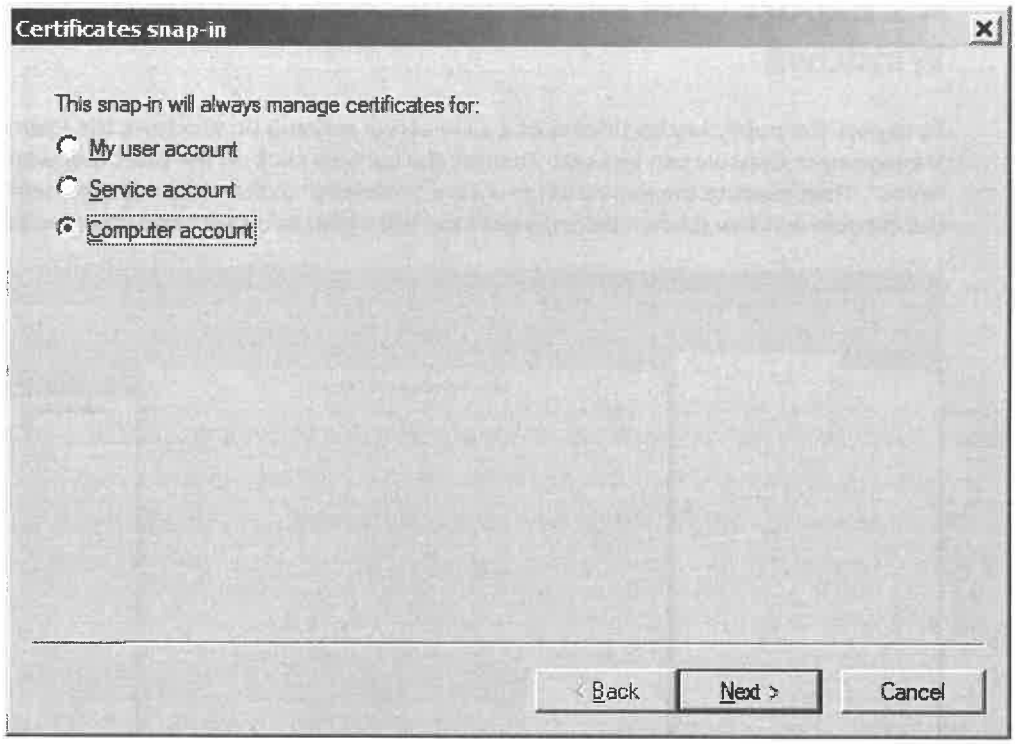
11.1 A.1 Export CAM server public key certificate on Windows

To export the public key certificate of a CAM server running on Windows the Microsoft Management Console can be used. To start the console click on the Start menu and search for "mmc". Then execute the appearing program "mmc.exe" to start the management console. In the console window (shown below) select the File menu and click "Add/Remove Snap-in...".

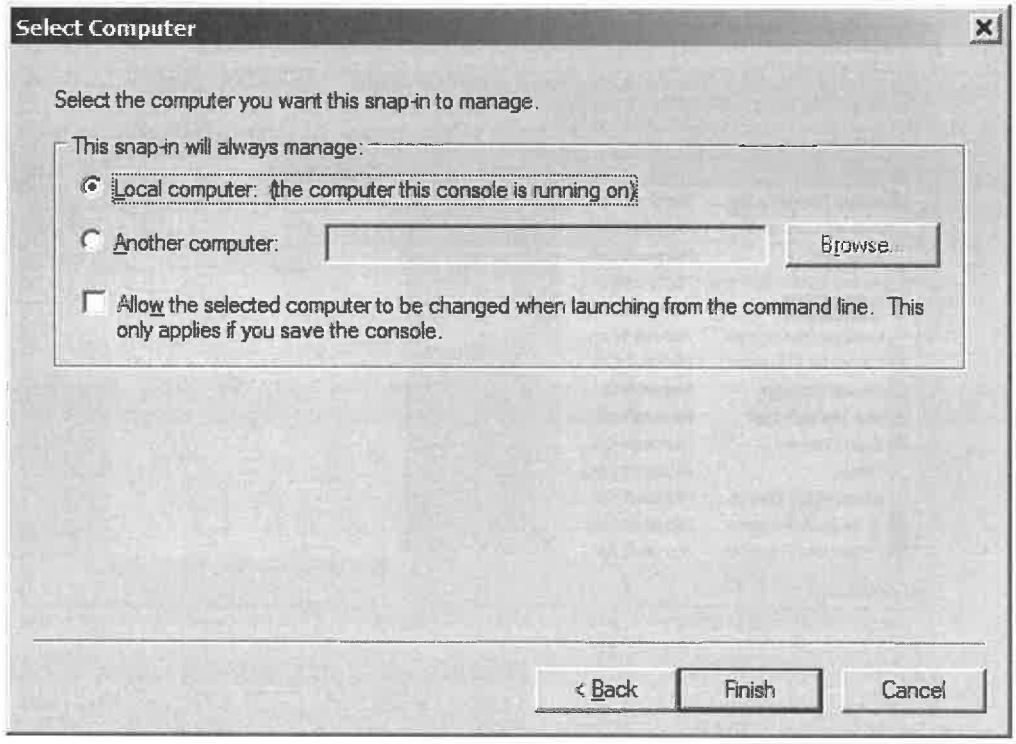
In the dialog "Add or Remove Snap-ins" select "Certificates" from the available snap-ins. The click "Add >" to start the certificate snap-in wizard dialog.



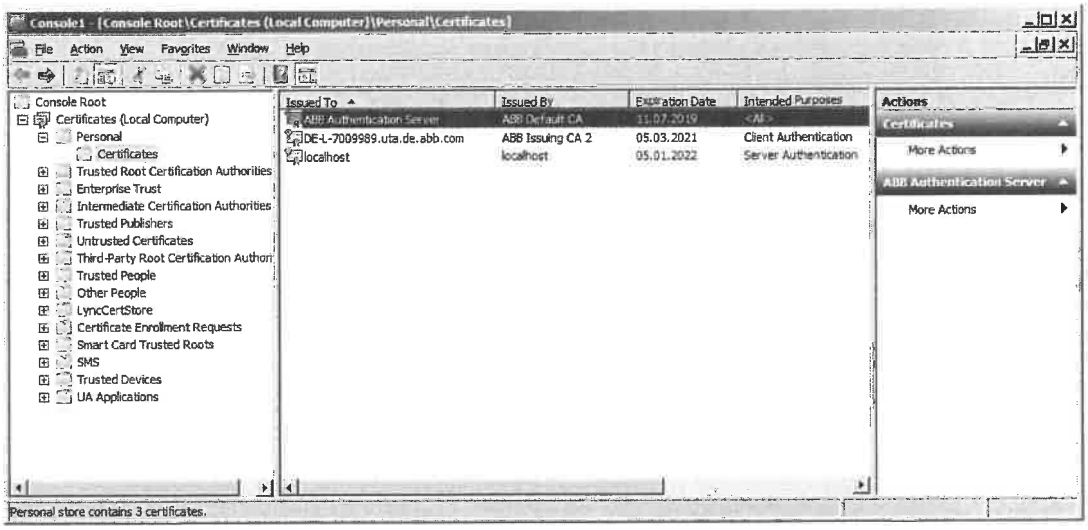
At first select for the certificates to manage by the snap-in the "Computer account" as shown in the next figure.



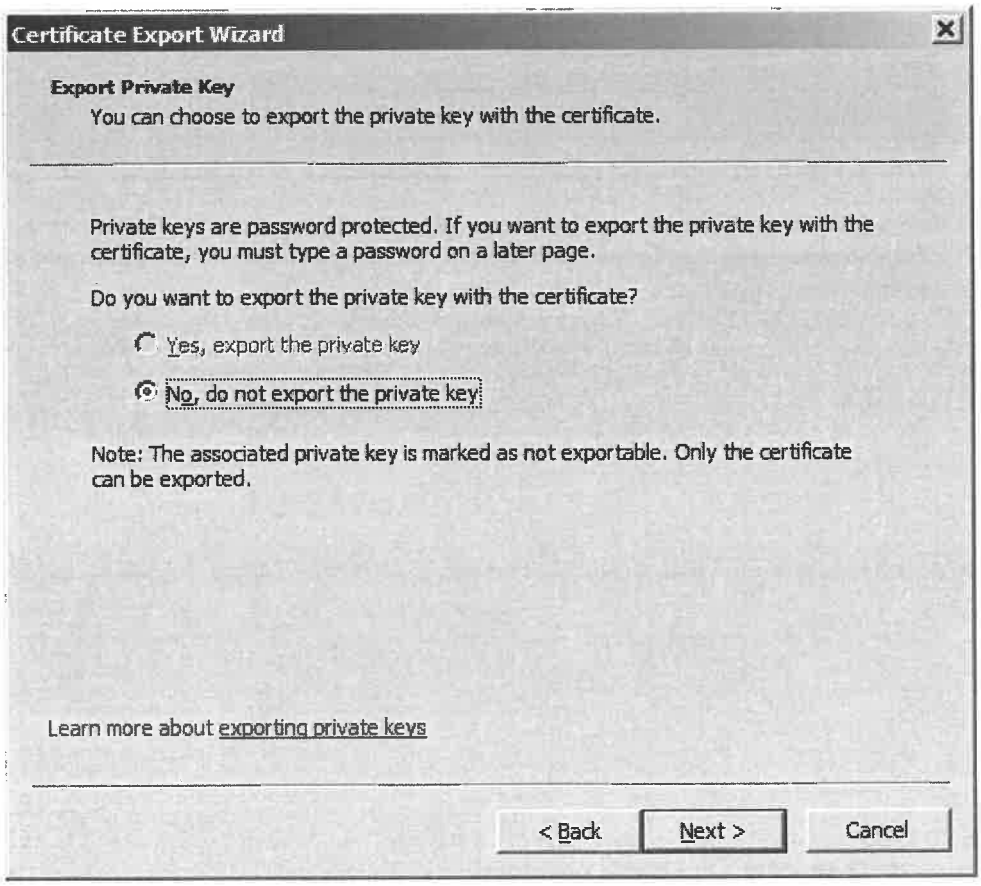
As computer for the certificate snap-in select the "Local computer (the computer this console is running on)". Then press "Finish" in the wizard and "Ok" in the dialog "Add or Remove Snap-ins".



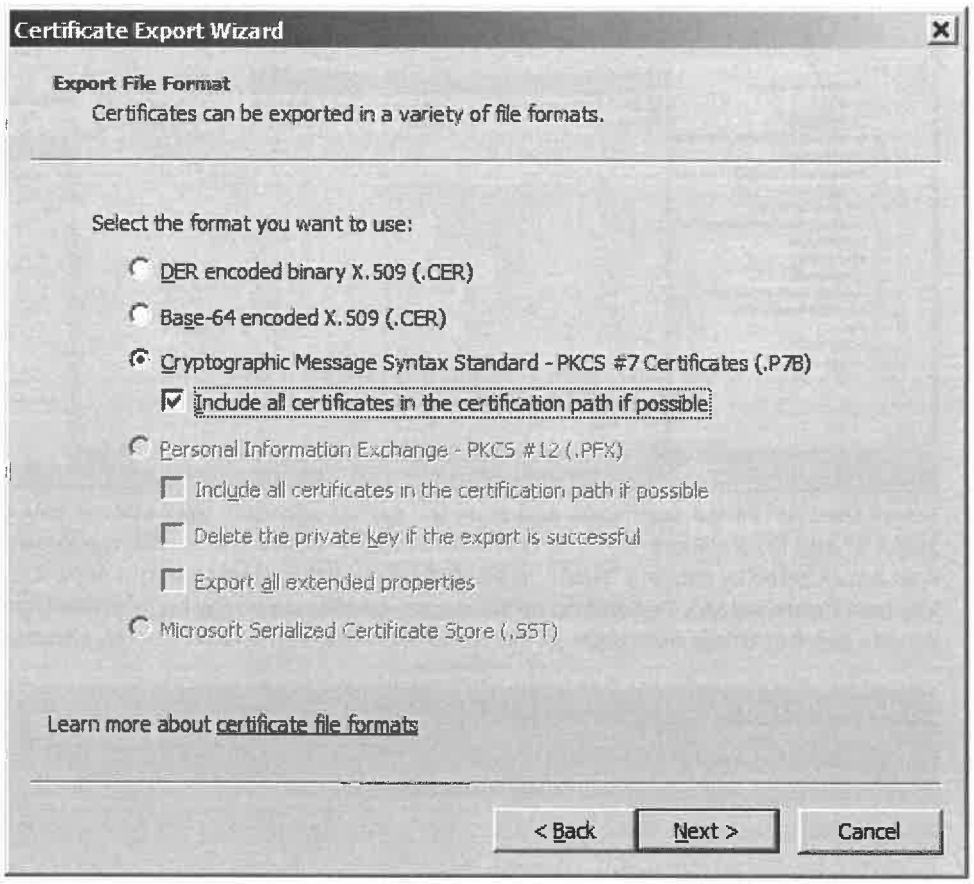
Now the management console shows the different certificate stores on the local computer. The certificate of the CAM server should be found in the Personal store (see next figure).



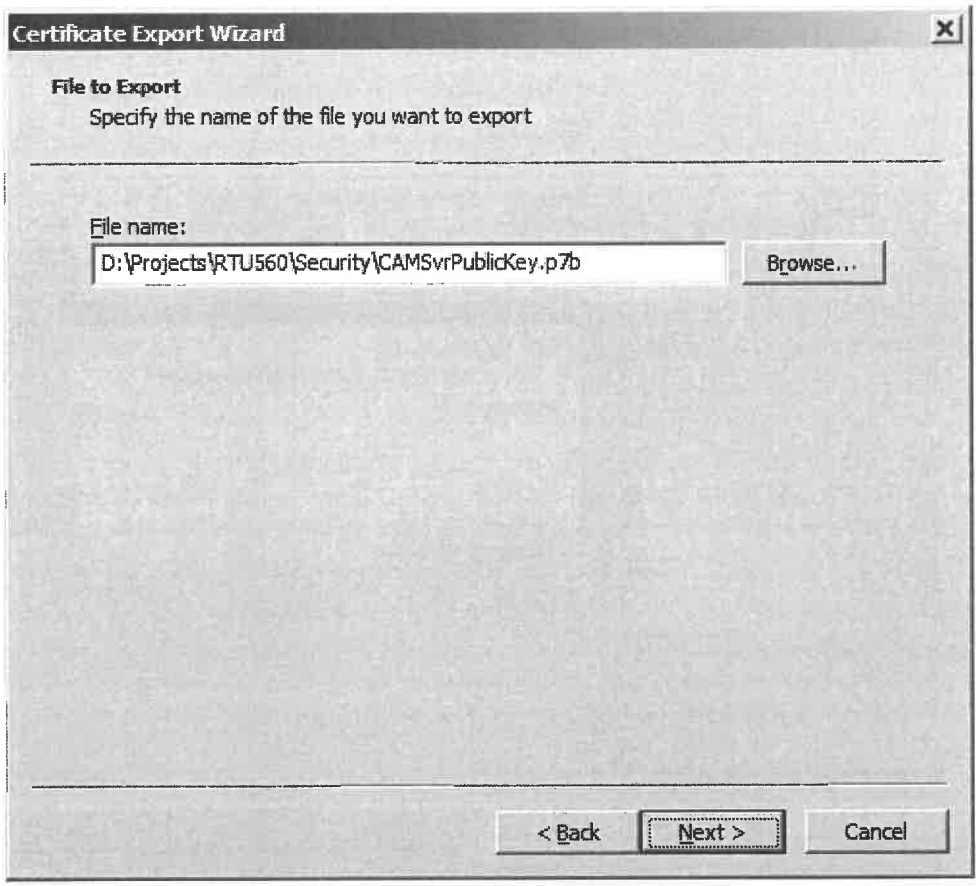
Select the CAM server certificate and start the export wizard in the Action menu, then "All Tasks >" and finally "Export...". The certificate export wizard starts with a welcome dialog that are skipped by clicking "Next". In the following dialog choose to not export the private key (see figure below). Depending on the server certificate it may be possible to export the private key, but this is not required. Continue with the next wizard step by clicking "Next".



In the next wizard step select the export format "Cryptographic Message Syntax Standard – PKCS#7 Certificates (.P7B)". The certification path must be exported. So, make sure to set the according check box as shown below. Continue with the next wizard step by clicking "Next".



In the following wizard step define the name of the file to export. Be sure that the extension of the export file is "*.p7b" (see next figure). Then continue with the next wizard step by clicking "Next".



In the final step of the export wizard an overview about the specified parameter are shown (see below). Check the configuration for correctness and press the button "Finish" to start the certificate export. If successful the resulting file containing the CAM server public key certificate, can be uploaded to the RTU500 series.


Certificate Export Wizard
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name D:\Proj
Export Keys No
Include all certificates in the certification path No
File Format Crypto
< Back
Finish
Cancel

12 Glossary

AD	Active Directory
AES	Advanced Encryption Standard
CAM	Central User Account Management
CF	Compact Flash
CMU	Communication and Data Processing Unit
DC	Direct Current
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DH	Diffie–Hellman key exchange
DO	Digital Output
IED	Intelligent Electronic Device
IKE	Internet Key Exchange
LAM	Local User Account Management
LDAP	Lightweight Directory Access Protocol
NCC	Network Control Center
NIST	National Institute of Standards and Technology
PC	Personal Computer
PLC	Programmable Logic Control
PPP	Point to Point Protocol
RFC	Request for Comments
RTU	Remote Terminal Unit
SCADA	Supervision, Control and Data Acquisition
SD	Secure Digital Memory Card
SEV	System Event
SHA	Secure Hash Algorithms
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol (according to RFC 4330)
TCP/IP	Transmission Control Protocol / Internet Protocol
TDEA	Triple Data Encryption Algorithm
UAM	User Account Management
UDP	User Datagram Protocol
USB	Universal Serial Bus

VPN	Virtual Private Network

Note:

The specifications, data, design or other information contained in this document (the "Brochure") - together: the "Information" - shall only be for information purposes and shall in no respect be binding. The Brochure does not claim to be exhaustive. Technical data in the Information are only approximate figures. We reserve the right at any time to make technical changes or modify the contents of this document without prior notice. The user shall be solely responsible for the use of any application example or information described within this document. The described examples and solutions are examples only and do not represent any comprehensive or complete solution. The user shall determine at its sole discretion, or as the case may be, customize, program or add value to the ABB products including software by creating solutions for the end customer and to assess whether and to what extent the products are suitable and need to be adjusted or customized.

This product is designed to be connected to and to communicate information and data via a network interface. It is the users sole responsibility to provide and continuously ensure a secure connection between the product and users or end customers network or any other network (as the case may be). The user shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB AG is not liable for any damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

ABB AG shall be under no warranty whatsoever whether express or implied and assumes no responsibility for the information contained in this document or for any errors that may appear in this document. ABB AG's liability under or in connection with this Brochure or the files included within the Brochure, irrespective of the legal ground towards any person or entity, to which the Brochure has been made available, in view of any damages including costs or losses shall be excluded. In particular ABB AG shall in no event be liable for any indirect, consequential or special damages, such as – but not limited to – loss of profit, loss of production, loss of revenue, loss of data, loss of use, loss of earnings, cost of capital or cost connected with an interruption of business or operation, third party claims. The exclusion of liability shall not apply in the case of intention or gross negligence. The present declaration shall be governed by and construed in accordance with the laws of Switzerland under exclusion of its conflict of laws rules and of the Vienna Convention on the International Sale of Goods (CISG).

Visit us

ABB AG
Power Grids
P.O. Box 10 03 51
68128 Mannheim, Germany

www.abb.com/remote-terminal-units

1KGT 150 925 V005 1

Документ 4.16.

Изчислената по дадената в Приложение 8 от раздел I от документацията за участие методика разполагаемост на всяка от предложените конфигурации.

Обобщени резултати от извършени изчисления на надеждността и разполагаемостта на Remote Terminal Unit (RTU) устройствата за нуждите на ЦДУ

Модул/MTBF/R			RTU Голям	RTU Малък	SAS комуникационен сървър
Модул тип	$MTBF_i$ (h)	R_i при SMT=87000h	Бр. модули	Бр. модули	Бр. модули
560CMR02	1034324	0.919	2	2	4
560PSR00	512612	0.844	6	4	2
560BIR01 R0001	1899526	0.955	25	17	2
560BOR01	11264255	0.992	3	3	1
560AIR01 R001	1853134	0.954	10	5	2
23AA21	1223404	0.931	2	2	0
560SFR02	5068696	0.983	3	2	1
560BCU05	2657492	0.968	1	1	3
CP-E 24/2.5	520000	0.846	3	2	1
Надеждност на RTU Средно време между повредите на RTU (h) Разполагаемост на RTU при MTTR=12h			R_{RTU}=0.953 $MTBF_{RTU}$=1 807 215 A_{RTU}=**0.9999934**	R_{RTU}=0.934 $MTBF_{RTU}$=1 274 187 A_{RTU}=**0.9999906**	R_{RTU}=0.803 $MTBF_{RTU}$=396 535 A_{RTU}=**0.9999889**
$R_i=e^{-SMT/MTBFi}$			$R_{RTU}=R_1R_2...R_n*((1-(1-R_1)(1-R_2)...(1-R_m))$ за n последователно свързани елементи и m паралелно свързани елементи $MTBF_{RTU}=SMT/\lvert \ln(R_{RTU}) \rvert$ $A_{RTU}=MTBF_{RTU}/MTBF_{RTU}+MTTR$ MTTR=средно време за отстраняване на повредата=12h, клас M3 (IEC 60870-4) SMT=87000h		

АББ България ЕООД
Централен офис
бул. „Витоша" № 895
Милениум център, сграда А, ет. 17
София 1408, България
Тел.: +359 (0) 2 807 55 00
Факс: +359 (0) 2 807 55 99
Web: **www.abb.bg**
E-mail: **office@bg.abb.com**

ЕИК: 831133152
ДДС номер: BG 831133152
Банкови данни:
ИНГ Банк, клон София
IBAN: BG13INGB91451000027317 (BGN)
IBAN: BG60INGB91451400027311 (EUR)
BIC: INGBBGSF

08.2017

Документ 4.17.

Описание на фирмената политика на Производителя за жизнения цикъл на предлаганите изделия и на частите за тяхната поддръжка

ABB AG - Power Systems Division • Postfach 10 03 51 • 68128 Mannheim

Person in charge
Ulrich Fuhrmann

Phone
+49 621 381- 3692

Fax
+49 621 381- 7101

E-Mail
Rtu-sales-support@de.abb.com

Our ref. (please quote)
PSNM-PS-UFu, Product Lifecycle RTU general 2017.docx

Your reference

Your letter dated

Date
April 1, 2017

GENERAL CONFIRMATION

ABB applies a specific policy for public announcement of products leaving the "active" status to become "classic", "limited" and finally "obsolete".

Once an ABB product enters in "classic phase", according to ABB policy, it is supported for service, replacement and limited improvement for 10 years at least.

The detailed policy description is presented on the following page.

The RTU500 series with the product lines RTU560, RTU540 and RT520 are not reported entering in "classic phase" for 2017. There is continuous development on existing and future RTU500 series.

Further: products reported in the currently valid published RTU price list are considered still in active phase. Only a few products from that pricelist are marked classic/limited and a remainder of stock is available. RTU500 series items are listed in price lists for 2017 and accordingly are still in active phase.

Mannheim, 01.04.2017

Заличено по чл. 36а, ал.3 от ЗОП

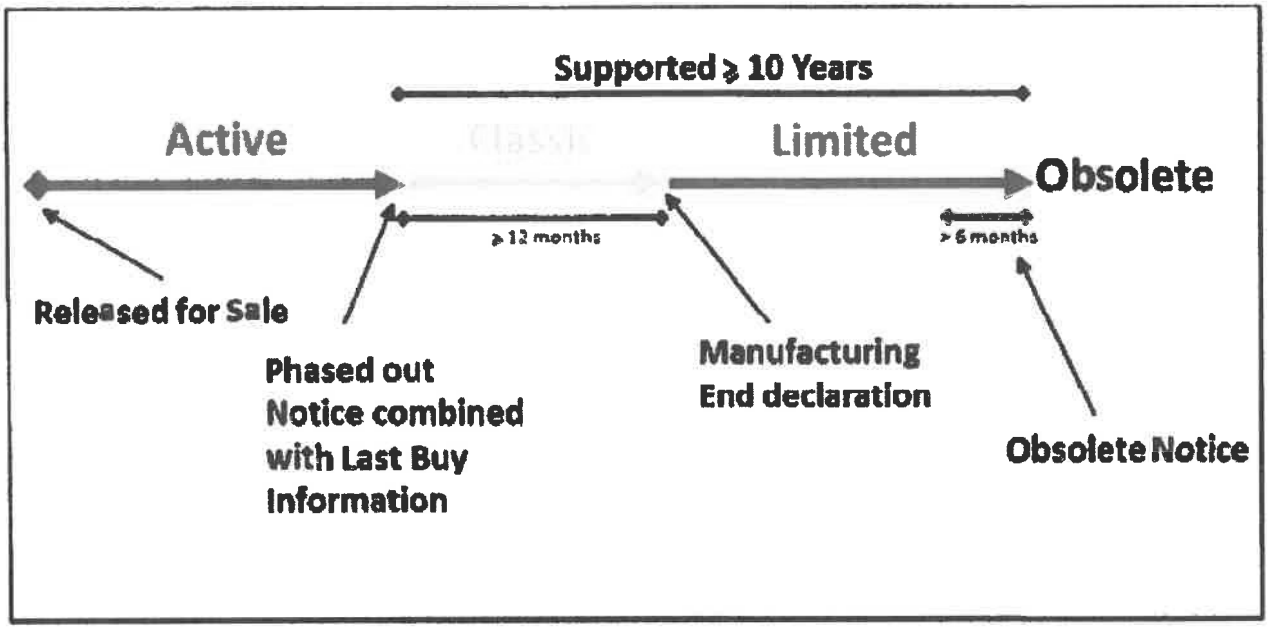
i.A. Sigbert Reimann

RTU Product Manager
Grid Automation Products
ABB AG

Заличено по чл. 36а, ал.3 от ЗОП

i.V. Thorsten Platz

Head of RTU Sales
Grid Automation Products
ABB AG



Lifecycle Policy Statement

The lifecycle policy statement forms the ABB Substation Automation Products commitment:

Products from ABB's Substation Automation Products are designed for continuous evolution. It is ABB's goal to protect our customers' investment beyond the lifecycles of the underlying platform products (i.e. hardware and software).

ABB will not phase out any product or "family" of products until an equivalent replacement to those products are available. Exceptions to this may occur if components or technologies needed are no longer available to ABB.

Once a product has been removed from active sales it is moved to the Classic phase. A Classic product will be phased out, minimum 12 months prior to any "Manufacturing End Declaration". ABB will announce the phase out and a "Last Buy" opportunity (expect in cases where there is a direct replacement).

Once a product has been phased out, it will move into the Limited phase. It is ABB's intention to provide support for as long as there is significant customer needs after the "Manufacturing End" through field service, repair and by making replacement spares (new or refurbished modules) available.

ABB will continue to support the products for at least 10 years, from the start of the Classic phase, although exceptions to this may occur if components or technologies are no longer available to ABB.