A1 - Release notes

Installing the APROL system (APROL R4.2)

Version: **V7.08 (2019-01-21 10:18:25)**

All values in this manual are current as of its creation. We reserve the right to change the contents of this manual without notice. B&R Industrial Automation GmbH is not liable for technical or editorial errors and defects in this manual. In addition, B&R Industrial Automation GmbH assumes no liability for damages that are directly or indirectly attributable to the delivery, performance or use of this material. We point out that the software and hardware designations and brand names of the respective companies used in this document are subject to general trademark, brand or patent protection.

1 APROL R4.2-05 release notes

1.1 Increasing safety

As part of regular APROL system security reviews, various changes and corrections that significantly increase the system security were performed.

In addition to the common security improvements listed below, all Linux packages are cyclically analyzed for possible vulnerability and supplied in an updated version on a separate AutoYaST DVD.

> **Information:**
>
> **For additional information about Security in APROL (overview), see the chapter of the same name in manual "D6 - Security".**

Common security improvements

1. Disabling the FTP service

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

To increase system security, the FTP service that is classified as unsafe was **disabled** in AutoYaST V4.2-030 and later. This means that when newly installing the AutoYaST DVD, the FTP service is installed but **disabled by default**.

If the service is then explicitly enabled, the following restrictive basic settings apply:

- Anonymous access is disabled.
- Local users can log in but cannot leave the associated home directory.

> **Note:**
>
> **B&R recommends that you do not enable the FTP service for security reasons and use the Linux services SFTP or SCP for secure data transfer instead.**

2. Removing the finger service

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

To increase system security, the finger service that is classified as unsafe was **removed** from AutoYaST V4.2-030 and later. This means that neither the finger service nor the finger utility are installed when newly installing the AutoYaST DVD. When updating AutoYaST from an older installation, both packages are displayed in the list of packages to be deleted.

In addition, the TCP port associated with the finger service has been closed.

3. Regulation of SSH access

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

To increase system security in APROL R4.2-05 and later, SSH access via password for Linux superuser "root" has been blocked.

> **Note:**
>
> **This does not affect SSH access of the superuser using certificates.**

In addition, unsuccessful attempts to initiate an SSH connection will be logged for all Linux users. If ten unsuccessful attempts are made within three minutes, SSH access is blocked for ten minutes for the IP address from which the connection attempts were made.

4. Encryption of VNC access

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

To increase system security, VNC access will in future only be possible in encrypted form (using certificate X.509).

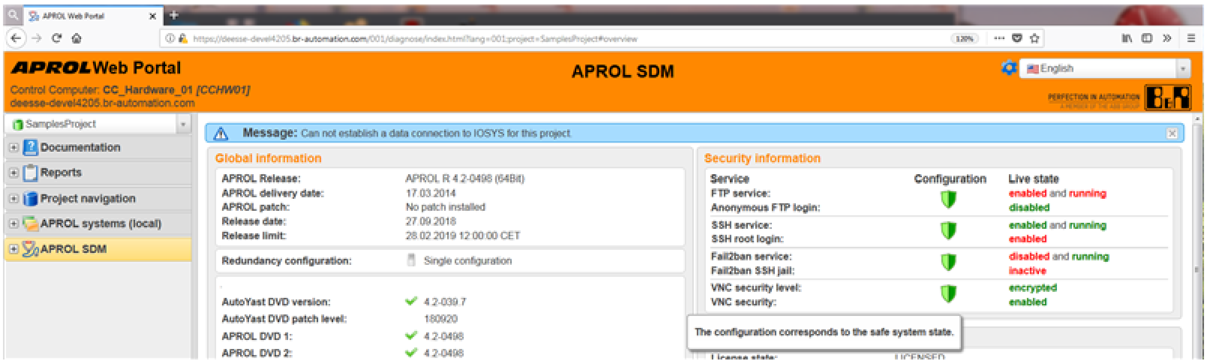
In APROL R4.2-05 and later, remote operation of an APROL server via the VNC protocol can only be performed via the B&R recommended client "TigerVNC". This applies to VNC access from both Windows and Linux environments.

> **Note:**
>
> **Connections via other VNC clients (e.g. RealVNC, UltraVNC or TightVNC) are no longer possible.**

Using utility `AprolSetSecurity`, the aforementioned services can be enabled or disabled.

> **Note:**
>
> **For detailed information about using the utility, use the call `AprolSetSecurity -help`.**

The current status of the aforementioned services is displayed in APROL SDM / area "Security information".



Control Computer: CC_Hardware_01 *[CCHW01]*
deesse-devel4205.br-automation.com

Message: Can not establish a data connection to IOSYS for this project.

Global information

APROL Release:	APROL R 4.2-0498 (64Bit)
APROL delivery date:	17.03.2014
APROL patch:	No patch installed
Release date:	27.09.2018
Release limit:	28.02.2019 12:00:00 CET
Redundancy configuration:	Single configuration
AutoYast DVD version:	✓ 4.2-039.7
AutoYast DVD patch level:	180920
APROL DVD 1:	✓ 4.2-0498
APROL DVD 2:	✓ 4.2-0498

Security information

Service	Configuration	Live state
FTP service: Anonymous FTP login:	🛡	enabled and running disabled
SSH service: SSH root login:	🛡	enabled and running enabled
Fail2ban service: Fail2ban SSH jail:	🛡	disabled and running inactive
VNC security level: VNC security:	🛡	encrypted enabled

The configuration corresponds to the safe system state.

License state: LICENSED

Figure 1: Security information in the APROL web portal

5. TbaseServer: Correction of memory access errors

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

Several memory access issues in the TbaseServer have been fixed to reduce vulnerability to attacks. Additional pointer checks were also implemented.

6. LDAP server: Blocking anonymous access

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

Until now, it was possible to read data stored on the LDAP server (except passwords) via anonymous access to the LDAP server. This is no longer possible.

7. Solution EnMon: Removing possibility of SQL injection

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

A PHP script was vulnerable to SQL injections, allowing the user to "smuggle in" arbitrary SQL commands. This vulnerability was removed

8. Web scripts: Protecting against remote execution

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

Some web scripts allowed execution of arbitrary unwanted commands on the web server. This possibility was removed in all scripts

9. IosHttp: Encrypted modification of PVs via IosHttp interface

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

PVs could be changed unencrypted using the IosHttp service and the JSON interface. Access is now exclusively via an encrypted connection.

10. AprolLoader: Protecting against remote execution

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

The AprolLoader could be used to execute arbitrary unwanted commands via special attack scenario. This possibility was removed

11. AprolSqlServer: Closing various security vulnerabilities

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

The following security holes have been closed in the AprolSqlServer:

1. Ability to execute arbitrary commands,
2. Access to directories outside the working directory,
3. Bypassing authentication

The following security hole was closed in the SimbaEngine SDK that is used in the AprolSqlServer:

- Insufficient authentication options and memory leaks

12. Script "AprolCluster": Removing possibility of command injection

> **Note:**
>
> **Credit: Independently found by Positive Technologies**

Arbitrary commands could be introduced using Python script via script "AprolCluster" that is called with the functionality "sudo" and thus executed with root rights. This possibility was removed

1.2 ANSL authentication for accessing the controller

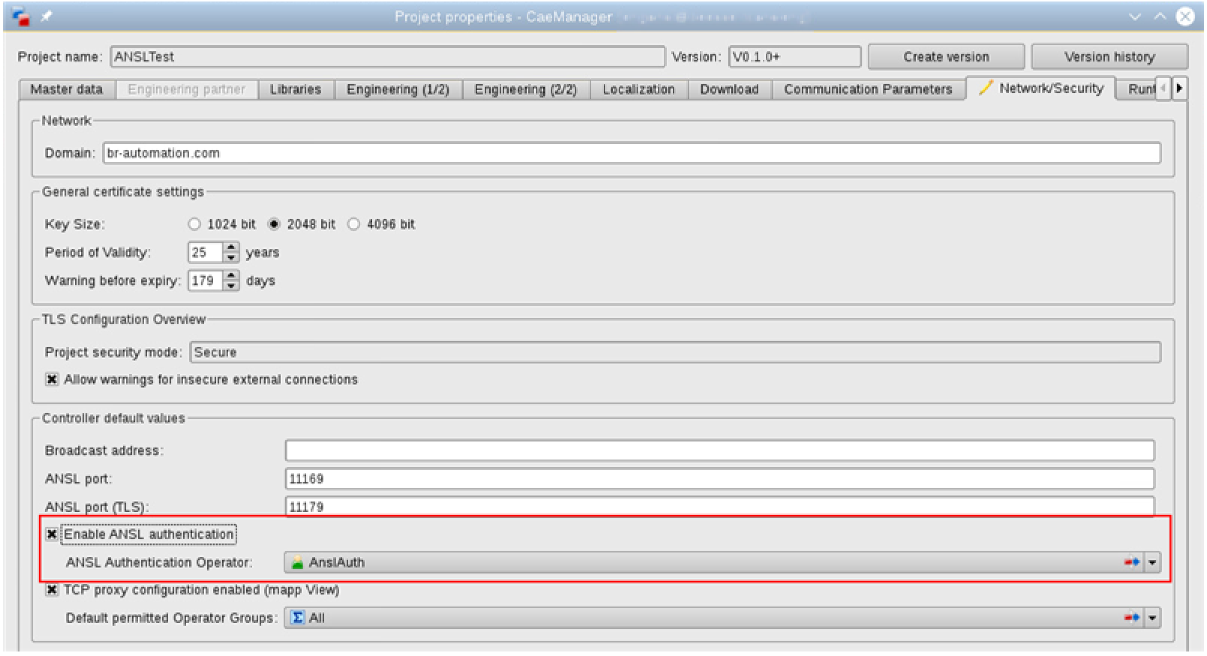
In AR OS version x0451 and later, ANSL authentication can be used to access SG4 controllers.

This can further enhance security, which was already significantly increased by support of a secure communication channel based on APROL TLS.

ANSL authentication for accessing the controller has the following benefits:

- ANSL communication with a B&R target system exclusively for selected operators
- Protection of B&R systems against unwanted access via ANSL

> **Information:**
>
> **For detailed information about ANSL authentication, see the chapter of the same name in manual "D6 - Security".**



Project name: ANSLTest

Version: V0.1.0+

Network

Domain: br-automation.com

General certificate settings

Key Size: ○ 1024 bit ● 2048 bit ○ 4096 bit

Period of Validity: 25 years

Warning before expiry: 179 days

TLS Configuration Overview

Project security mode: Secure

☒ Allow warnings for insecure external connections

Controller default values

Broadcast address:

ANSL port: 11169

ANSL port (TLS): 11179

☒ Enable ANSL authentication

ANSL Authentication Operator: AnslAuth

☒ TCP proxy configuration enabled (mapp View)

Default permitted Operator Groups: Σ All

Figure 2: Configuring ANSL authentication in the project properties

1.3 APROL TLS: Secure connections with Transport Layer Security

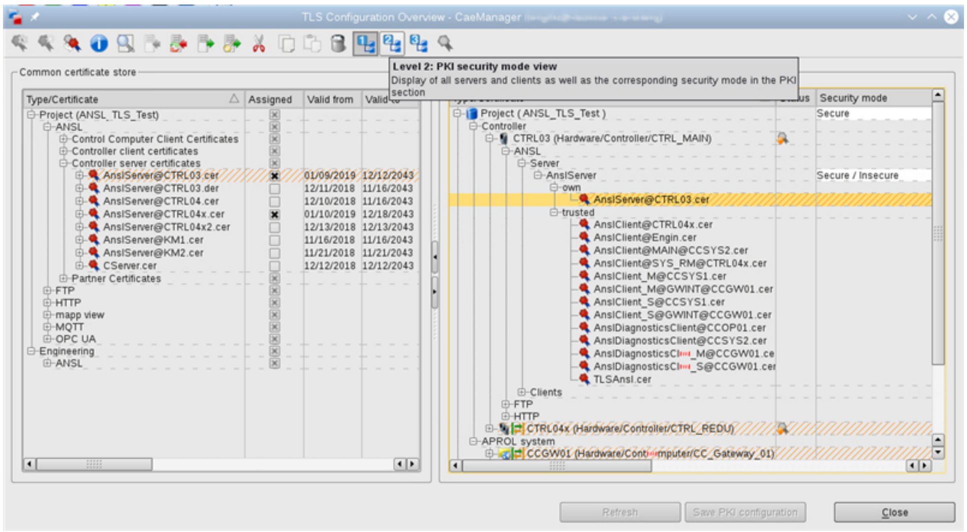
In APROL R4.2-05 and later, all servers and clients can be switched over to secure communication using TLS in one central place by means of fast and convenient configuration.

> **Information:**
>
> **For detailed information about APROL TLS, see the chapter of the same name in manual "D6 - Security".**

The certificates required for encrypted communication between servers and clients in an APROL project can be created automatically in the CCS (Common Certificate Store) and assigned in the same step to the corresponding instances in the PKI configuration.

Certificates required to communicate with external communication partners can be imported into the CCS and manually assigned to the PKI configuration.

The central dialog box for configuring TLS encryption, "TLS configuration overview", can be accessed in the CaeManager via menu "Tools".



Level 2: PKI security mode view
Display of all servers and clients as well as the corresponding security mode in the PKI section

Type/Certificate	Assigned	Valid from	Valid to
Project (ANSL_TLS_Test)	☒		
ANSL	☒		
Control Computer Client Certificates	☒		
Controller client certificates	☒		
Controller server certificates	☒		
AnslServer@CTRL03.cer	☒	01/09/2019	12/12/2043
AnslServer@CTRL03.der	□	12/11/2018	11/16/2043
AnslServer@CTRL04.cer	□	12/10/2018	11/16/2043
AnslServer@CTRL04x.cer	☒	01/10/2019	12/18/2043
AnslServer@CTRL04x2.cer	□	12/13/2018	12/13/2043
AnslServer@KM1.cer	□	11/16/2018	11/16/2043
AnslServer@KM2.cer	□	11/21/2018	11/21/2043
CServer.cer	□	12/12/2018	12/12/2043
Partner Certificates	☒		
FTP	☒		
HTTP	☒		
mapp view	☒		
MQTT	☒		
OPC UA	☒		
Engineering	☒		
ANSL	☒		

Type/Certificate	Status	Security mode
Project (ANSL_TLS_Test)		Secure
Controller		
CTRL03 (Hardware/Controller/CTRL_MAIN)		
ANSL		
Server		
AnslServer		Secure / Insecure
own		
AnslServer@CTRL03.cer		
trusted		
AnslClient@CTRL04x.cer		
AnslClient@Engin.cer		
AnslClient@MAIN@CCSYS2.cer		
AnslClient@SYS_RM@CTRL04x.cer		
AnslClient_M@CCSYS1.cer		
AnslClient_M@GWINT@CCGW01.cer		
AnslClient_S@CCSYS1.cer		
AnslClient_S@GWINT@CCGW01.cer		
AnslDiagnosticsClient@CCOP01.cer		
AnslDiagnosticsClient@CCSYS2.cer		
AnslDiagnosticsCl_M@CCGW01.ce		
AnslDiagnosticsCl_S@CCGW01.cer		
TLSAnsl.cer		
Clients		
FTP		
HTTP		
CTRL04x (Hardware/Controller/CTRL_REDU)		
APROL system		
CCGW01 (Hardware/Cont mputer/CC_Gateway_01)		

Figure 3: Dialog box "TLS configuration overview"

1.4 mapp View in APROL

With mapp View, B&R supports convenient development – based on modern web technology – of HMIs for B&R automation applications.

The technical basis of mapp View is *HTML5, CSS3* and the scripting language *JavaScript* (JS). Since these web technologies are encapsulated in visualization elements (widgets) provided by B&R, no detailed knowledge is required.

This allows application developers to concentrate fully on their core competency.

Benefits of the mapp View HMI

The B&R mapp View HMI offers the following benefits:

- OPC UA as the data management basis
- Simple implementation of data sources from third-party manufacturers into the controller HMI applications
- Platform-independent, quick and convenient creation of web-based HMI applications

- Investment protection through use of the worldwide web standards *HTML5, CSS3* and *JavaScript*
- Increase in productivity and reduction of downtime through use of efficient and intuitive operation
- Optimal reusability due to independent content and layout of the HMI application as well as HMI elements and machine logic

Supporting mapp View HMI applications in APROL

The creation of a web-based HMI application with mapp View is currently supported to a reduced extent in the APROL system environment.

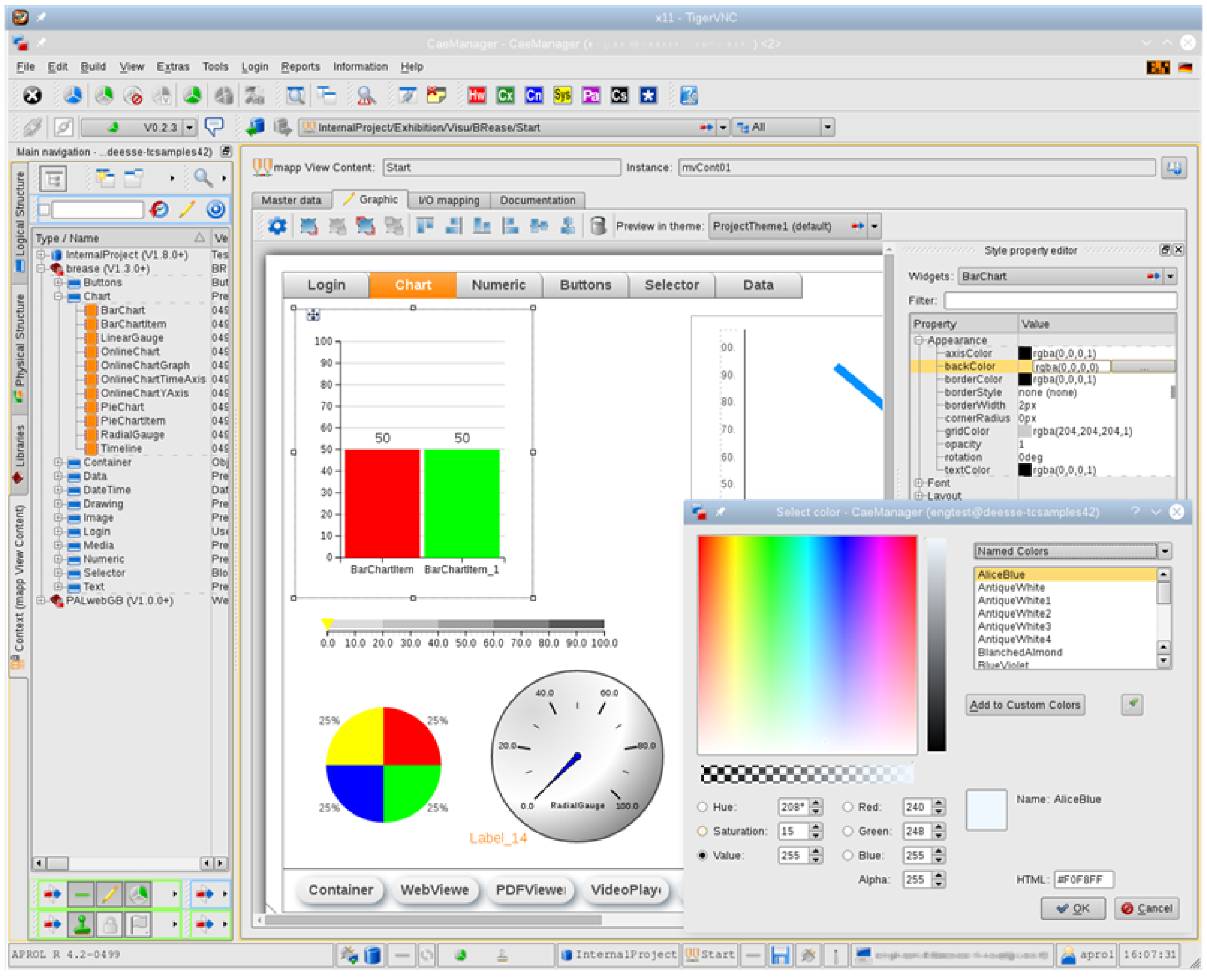
> ### Important!
>
> **For the existing Limitations in the current APROL release, see the chapter of the same name in manual "A3 - Upgrade notes".**

The main focus of the integration of the mapp View technology was to base it on the proven workflow for creating a HMI application.

The visualization elements (widgets) are delivered in prepared CAE libraries and can be used in CAE projects in a similar manner as classic graphic blocks.

The HIM application is created in the CAE project using project part "mapp View content". The created HMI application can be assigned to a certain controller and is available as a separate page in the runtime environment after the subsequent build and download procedure.

> ### Information:
>
> **For detailed information about mapp View in APROL see the chapter of the same name in manual "B2 - Project engineering"**



mapp View Content: Start

Instance: mvCont01

Preview in theme: ProjectTheme1 (default)

Widgets: BarChart

Filter:

Property	Value
Appearance	
axisColor	■ rgba(0,0,0,1)
backColor	rgba(0,0,0,0)
borderColor	■ rgba(0,0,0,1)
borderStyle	none (none)
borderWidth	2px
cornerRadius	0px
gridColor	rgba(204,204,204,1)
opacity	1
rotation	0deg
textColor	■ rgba(0,0,0,1)
Font	
Layout	

○ Hue: 208°
○ Saturation: 15
● Value: 255
○ Red: 240
○ Green: 248
○ Blue: 255
Alpha: 255

Name: AliceBlue

HTML: #F0F8FF

Figure 4: mapp View content

1.5 Configuring AS hardware on an external Windows system

VMware workstation V14 or later can no longer be used to configure the AS hardware if the APROL system software is executed in a *Hyper-V* environment or with the *B&R Hypervisor*.

In the aforementioned cases or to relieve the local *VMware* on an engineering server, *Automation Studio* can now also be used on an external *Windows* system or in a *VMware* on an external server .

Communication between the APROL engineering system (CaeManager) and the external *Windows* system (*Automation Studio*) is now carried out via an AprolRemoteExecServer installed on the *Windows* system.

Point-to-point encryption is used to secure the communication and guarantee authentication and encryption of the communication.

> **Note:**
>
> **In this context, note the instructions in chapter "AS hardware configuration on an external Windows system" of manual "A3 - Upgrade notes".**

1.6 Client DA modules for configuring OPC UA communication with external OPC UA servers

Separate block types are provided for efficient and reusable configuration communication between OPC UA clients (UaRClient) of the APROL systems and external OPC UA servers.

In contrast to "OPC-UA client coupling I/Os", it is possible to place and configure the separately provided blocks in a simple manner directly in hyper macros, for example.

Thus, in the CFC logic, the OPC UA data can thus be read or written directly where it is generated or required by instantiating these blocks in the CFC logic without using additional coupling I/Os. In addition, it is possible to use the described blocks to store parts of the OPC UA communication in hyper macros to enable simple reusability.

> **Information:**
>
> **For detailed information, see chapter "Client DA blocks for configuring OPC UA communication with external OPC UA servers" of manual "F1 - Drivers for B&R couplings".**

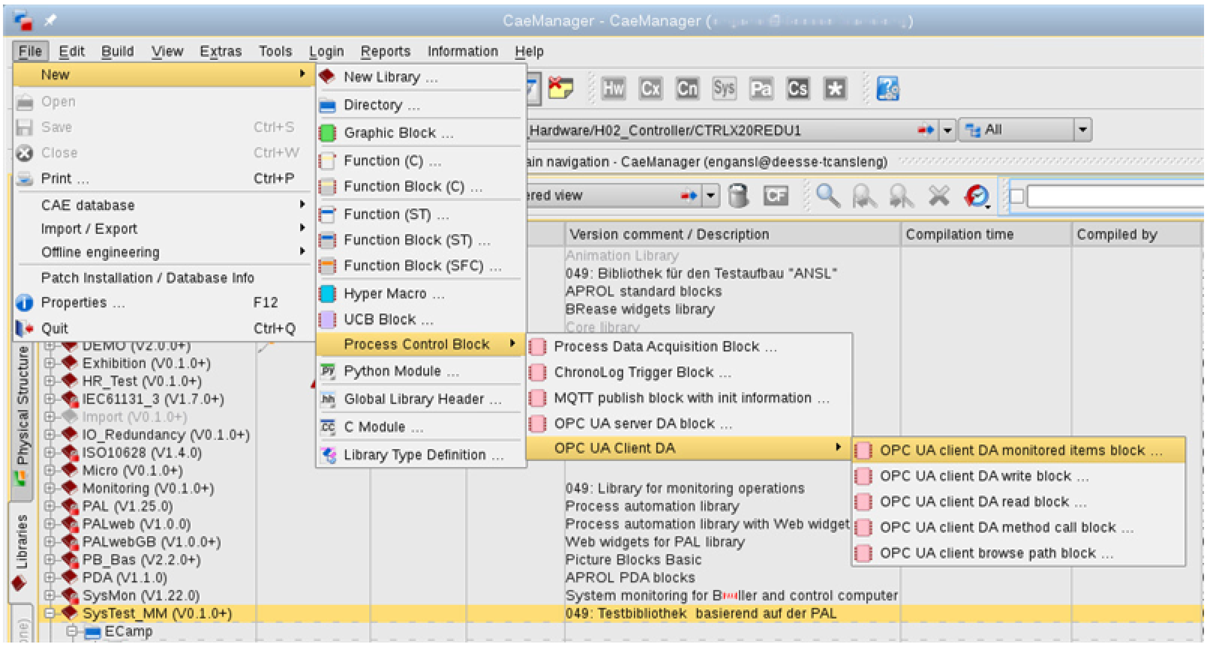


Figure 5: Creating a client DA block

1.7 Temporary text mode for convenient editing of texts in CFC and SFC

"Temporary text mode" enables you to edit text objects in CFC and SFC in a targeted way.

This mode is particularly useful if a large number of text objects are covered by other CFC objects (blocks, connections) when placed in the background of a CFC. This mode can be switched on or off via shortcut menu option "Temporary text mode". In text mode, only text objects are displayed in the specified color; all other objects are displayed in darkened and unsaturated colors.

> **Note:**
>
> **This temporary editing mode is switched off after closing the CFC or SFC editor. This mode is temporarily disabled while a CFC/SFC is being debugged.**

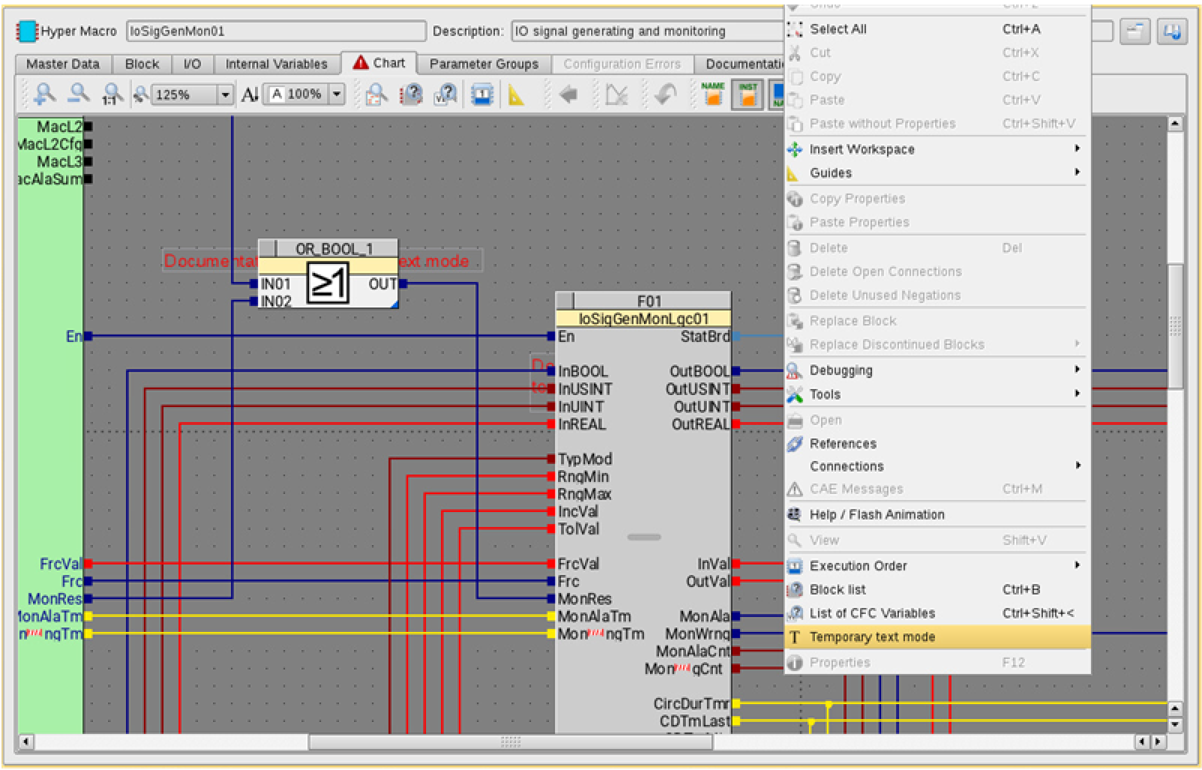


Figure 6: Temporary text mode 1/2

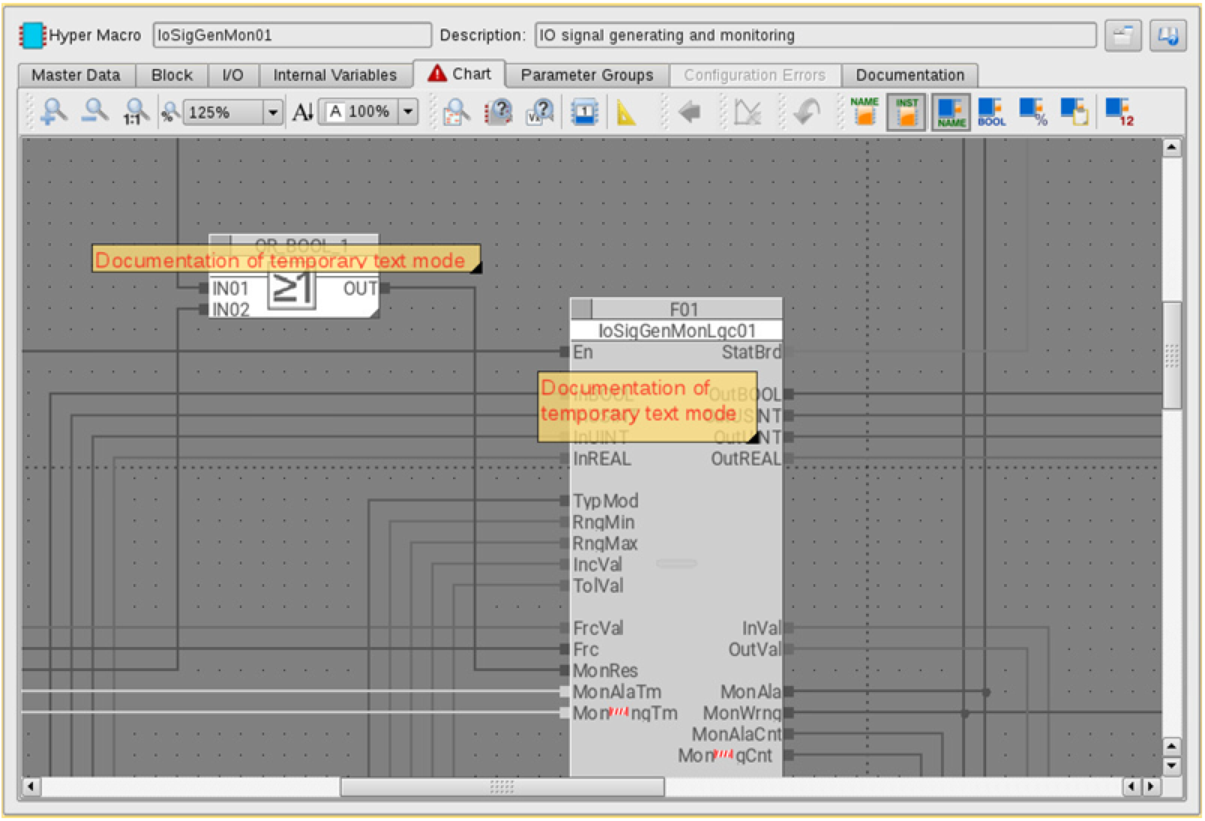


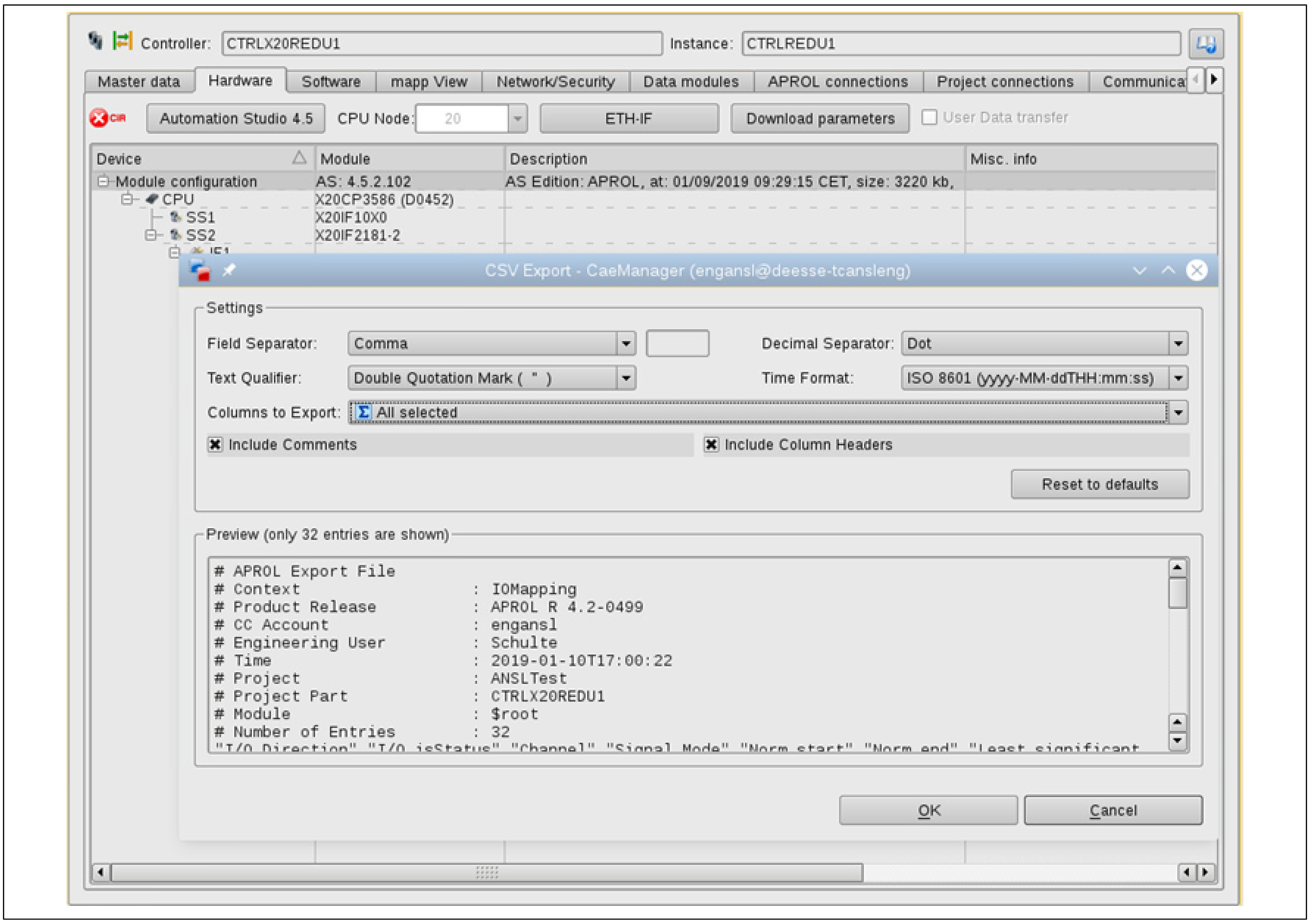
Figure 7: Temporary text mode 2/2

1.8 Export I/O mapping (CSV)

The data of the I/O mapping of individual modules or all modules could previously only be exported in the internal format. A CSV export can now be carried out in tab "Hardware" of project part "Controller" for all (or individual) I/O modules via shortcut menu option "Export I/O mapping (CSV)".

> **Note:**
>
> **The function is also available in the I/O mapping dialog box of an I/O module via a separate button.**

The export is controlled via a new central dialog box that allows numerous settings for the CSV format and also provides a preview of the CSV format. It is also possible to select separate columns to be included in the export.



Controller: CTRLX20REDU1 Instance: CTRLREDU1

Device	Module	Description	Misc. info
Module configuration	AS: 4.5.2.102	AS Edition: APROL, at: 01/09/2019 09:29:15 CET, size: 3220 kb,	
CPU	X20CP3586 (D0452)		
SS1	X20IF10X0		
SS2	X20IF2181-2		

CSV Export - CaeManager (engansl@deesse-tcansleng)

Settings

Field Separator: Comma

Decimal Separator: Dot

Text Qualifier: Double Quotation Mark (")

Time Format: ISO 8601 (yyyy-MM-ddTHH:mm:ss)

Columns to Export: Σ All selected

☒ Include Comments

☒ Include Column Headers

Preview (only 32 entries are shown)

```
# APROL Export File
# Context                   : IOMapping
# Product Release           : APROL R 4.2-0499
# CC Account                : engansl
# Engineering User          : Schulte
# Time                      : 2019-01-10T17:00:22
# Project                   : ANSLTest
# Project Part              : CTRLX20REDU1
# Module                    : $root
# Number of Entries         : 32
"I/O Direction" "I/O isStatus" "Channel" "Signal Mode" "Norm start" "Norm end" "Least significant
```

Figure 8: Export I/O mapping (CSV)

The selected configuration is saved user- and context-specific and is available once again for the next export of the same user, as "last used".

1.9 Supporting B&R hardware APC3100 and PPC3100

The APC3100 (already in APROL R4.2-03) and PPC3100 have been tested and validated for use in APROL R4.2 (based on SLE 12).

In this context, the APROL system service ApcHwInfo was extended to provide static and dynamic data for this B&R hardware.

These include static hardware revision information and BIOS information, as well as dynamic temperature data and runtime information that is updated regularly.

2 APROL R4.2-03 release notes

2.1 Validation of the B&R Automation PC 910 and 3100 with Trusted Platform Module

The B&R APC 910 and APC 3100 – with support of the TPM 2.0 standard – have been tested and validated for use in APROL R4.2 (based on SLE 12).

The APC 910 and APC 3100 could be extended with basic security functions by using the **T**rusted **P**latform **M**odule chip.

The additional security functions are used for licensing and data protection, for example. In addition, the spread of malware can be detected and prevented.

The TPM chip secures passwords, keys and certificates and serves to identify and authenticate the operating system, the PC client and the user with regard to checking procedures.

2.2 Hardware-based login using RFID card reader ADMITTO

General information about usage

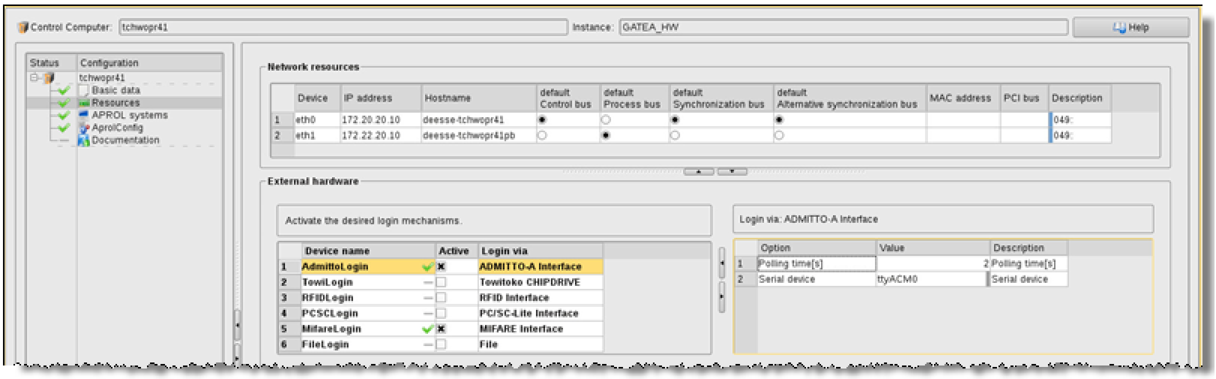
APROL supports hardware-based login using RFID card reader "ADMITTO-A-3100-D" with USB connection from the company *PHG*.

Requirements for use:

- The reader must be automatically registered by Linux system as /dev/ttyACMx (with x = 0 ... 3).
- The reader must be set so that it automatically forwards the UID of a scanned card.
- The active request of data from the card reader (mode "Active transmit") is not supported.
- The reader must be purchased from the manufacturer with corresponding configuration. Subsequent configuration using APROL tools is not possible.
- MIFARE systems with UIDs of 4, 7 and 10 bytes are supported.

Assigning hardware in the APROL system

In the CAE project, "AdmittoLogin" must be enabled under "Resources / Third-party hardware" for the operator station (in project part "Control computer") on which the hardware-supported login is to take place. A sampling rate of [2 ... 10] seconds can be configured for the LoginServer. This means that the LoginServer checks cyclically within the set time whether the card reader has detected a card.



Control Computer: tchwopr41
Instance: GATEA_HW

Status	Configuration
	tchwopr41
✓	Basic data
✓	Resources
✓	APROL systems
✓	AprolConfig
	Documentation

Network resources

	Device	IP address	Hostname	default Control bus	default Process bus	default Synchronization bus	default Alternative synchronization bus	MAC address	PCI bus	Description
1	eth0	172.20.20.10	deesse-tchwopr41	●	○	●	●			049:
2	eth1	172.22.20.10	deesse-tchwopr41pb	○	●	○	○			049:

External hardware

Activate the desired login mechanisms.

	Device name	Active	Login via
1	AdmittoLogin	✓ ☒	ADMITTO-A Interface
2	TowiLogin	— □	Towitoko CHIPDRIVE
3	RFIDLogin	— □	RFID Interface
4	PCSCLogin	— □	PC/SC-Lite Interface
5	MifareLogin	✓ ☒	MIFARE Interface
6	FileLogin	— □	File

Login via: ADMITTO-A Interface

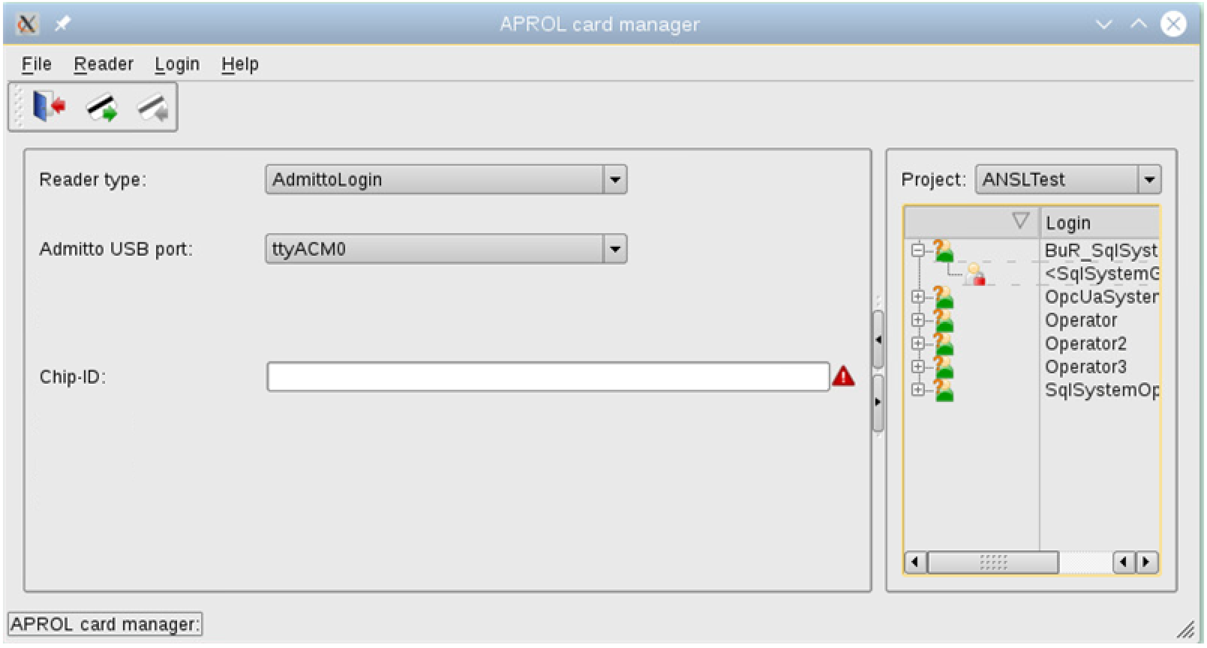
	Option	Value	Description
1	Polling time[s]	2	Polling time[s]
2	Serial device	ttyACM0	Serial device

Figure 9: Configuring the "AdmittoLogin" on the operator station

Reading the card UID

Use "KTowiTool" to determine the UID of the operator's RFID hardware. Utility "KTowiTool" for the administration of smart cards / transponders is located in the KDE start menu option "Tools / KTowiTool".

> ### Note:
>
> **To be able to read the UID of MIFARE cards, reader type "AdmittoLogin" was added to "KTowiTool".**



APROL card manager

Reader type: AdmittoLogin

Admitto USB port: ttyACM0

Chip-ID:

Project: ANSLTest

Login
BuR_SqlSyst
<SqlSystemG
OpcUaSyster
Operator
Operator2
Operator3
SqlSystemOp

APROL card manager:

Figure 10: Reading the card UID with "KTowiTool"

> ### Note:
>
> **Note that "KTowiTool" requires exclusive access to the reader. To be able to read or write smart cards on an operator system, all LoginServer processes must be stopped if the hardware login is already enabled!**

Utility "KTowiTool" is fully integrated into the APROL authorization system.

Within operator groups, the following application rights can be assigned for an operator:

- Start (start the application with read access)
- Edit (read and write access)

Assigning the card UID in the OperatorManager

In the OperatorManager in the context of the operator (tab "Login configuration" / "AdmittoLogin"), enter the previously determined UID in field "ID". Configure the hardware-based login using the additional options in entry "AdmittoLogin".

After "Build (configuration)" and subsequent download to the target systems, the operator login can be performed using the RFID hardware. Note that after initial configuration of "AdmittoLogin", the LoginServer on the target system must be stopped and restarted once.

The operator must either be logged out explicitly or automatically after the specified IDLE time has elapsed.

2.3 Configuring a firewall with IP address filtering

> **Information:**
>
> **For detailed information, see chapter "Configuring a firewall with IP address filtering" of manual "A2 - Getting started".**

It is possible to modify the firewall provided by SUSE in such a way that only certain remote computers are permitted to access the local computer.

This configuration is based on IP address filtering. APROL provides a mechanism to conveniently apply the whitelists previously put together by the system or network administrator. The APROL server can then only be accessed from the IP addresses contained in the whitelists. Note: The specified whitelist overwrites the default firewall configuration of APROL at the port level.

> **Note:**
>
> **The specified whitelist overwrites the default firewall configuration of APROL at the port level.**

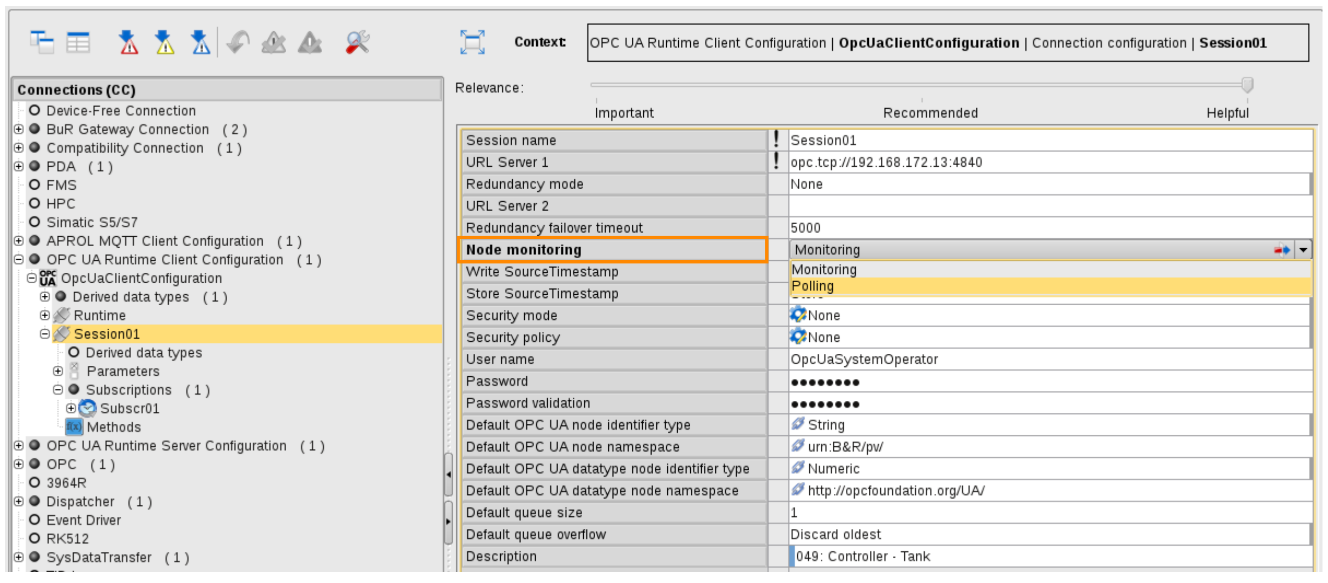
2.4 Configuration of polling access to OPC UA servers without monitoring support

> **Information:**
>
> **For information about open, standardized and vendor-independent communication via OPC UA, see chapter "OPC UA in APROL" of manual "F1 - Drivers for B&R couplings".**

Cyclic polling of nodes can be configured for communication with an OPC UA server that does not support subscriptions and therefore does not support node monitoring. Polling access is when the values of nodes are read at regular intervals via the service function of the session and values are post-processed as in monitoring.

> **Note:**
>
> **Servers with a limited range of functions are servers that only serve the "Nano embedded server" profile, for example.**

Cyclic polling is used in APROL coupling "OPC UA runtime client configuration" at the connection/**session** level via attribute "Node monitoring".



Context: OPC UA Runtime Client Configuration | **OpcUaClientConfiguration** | Connection configuration | **Session01**

Connections (CC)

- Device-Free Connection
- BuR Gateway Connection (2)
- Compatibility Connection (1)
- PDA (1)
- FMS
- HPC
- Simatic S5/S7
- APROL MQTT Client Configuration (1)
- OPC UA Runtime Client Configuration (1)
  - OpcUaClientConfiguration
    - Derived data types (1)
    - Runtime
    - Session01
      - Derived data types
      - Parameters
      - Subscriptions (1)
        - Subscr01
      - Methods
- OPC UA Runtime Server Configuration (1)
- OPC (1)
- 3964R
- Dispatcher (1)
- Event Driver
- RK512
- SysDataTransfer (1)

Session name	!	Session01
URL Server 1	!	opc.tcp://192.168.172.13:4840
Redundancy mode		None
URL Server 2		
Redundancy failover timeout		5000
Node monitoring		Monitoring Monitoring Polling
Write SourceTimestamp		
Store SourceTimestamp		
Security mode		None
Security policy		None
User name		OpcUaSystemOperator
Password		●●●●●●●●
Password validation		●●●●●●●●
Default OPC UA node identifier type		String
Default OPC UA node namespace		urn:B&R/pv/
Default OPC UA datatype node identifier type		Numeric
Default OPC UA datatype node namespace		http://opcfoundation.org/UA/
Default queue size		1
Default queue overflow		Discard oldest
Description		049: Controller - Tank

Figure 11: Polling access to OPC UA servers with limited range of functions

Division of the nodes into individual subscriptions including the associated configuration of the publishing interval remains unchanged.

> **Note:**
>
> **This allows a simple configuration change at any time if the OPC UA server is replaced by a server that supports monitoring, for example.**

The polling interval is set for each subscription via the publishing interval.

2.5 Receiving and writing the source timestamp

> **Information:**
>
> **For information about open, standardized and vendor-independent communication via OPC UA, see chapter "OPC UA in APROL" of manual "F1 - Drivers for B&R couplings".**

OPC UA supports the following timestamps for values:

- The source timestamp contains **the time of the last value change on the device or in the process database**, i.e. the data source.
- The server timestamp contains the **time at which the value from the data source is received by the OPC UA server**; this is the process database Iosys in APROL.

> **Important!**
>
> **Not all OPC UA servers support marking a node with one or both timestamps. Similarly, not all OPC UA servers accept the transfer of one or both timestamps when transferring value changes.**
>
> **Attempting to transfer a timestamp to an OPC UA server that does not accept a timestamp is acknowledged by the server with error "BadWriteNotSupported".**

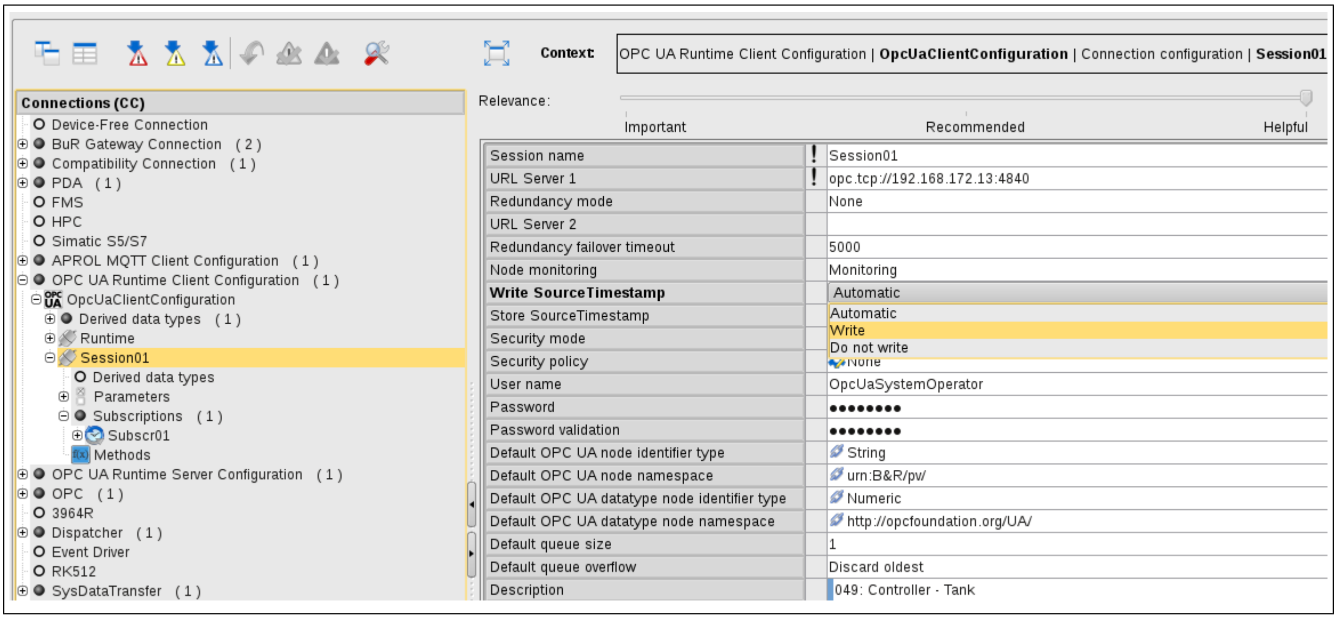
The receipt and writing of the source timestamp from the UaRServer or UaRClient is explained below:

Action:	Context: UaRServer
Provision of data	When providing values via a node in the address space of the server, the UaRServer offers the timestamp of the last value change in the process database Iosys as attribute *SourceTimestamp* of the node in addition to the current value. The source timestamp can be evaluated by an OPC UA client.
Reception of data	When an OPC UA client changes the value of nodes in the address space of the server, the UaRServer receives attribute *SourceTimestamp* and evaluates it. Valid timestamps are used as timestamps for the last value change when the value is transferred to the Iosys process database. This ensures that the exact time of the value change in the source is applied. This behavior is currently always active and cannot be configured. If no (valid) timestamp is transferred for attribute *SourceTimestamp*, the current time is used as the timestamp when the value is transferred to the process database Iosys. Transfer of the source timestamp to the process database can be prevented in project part "APROL system" under "System Services / UaRServer" by setting parameter "-rejectWriteSourceTS".

Table 1: UaRServer

Action	Context: UaRClient
Reception of data	When monitoring or reading values of nodes, a source timestamp transferred by the OPC UA server is evaluated by UaRClient and used as the timestamp of the last value change when transferring the value to the process database Iosys. If no source timestamp is transferred from the OPC UA server, the current time is used when writing the value to the process database. Transfer of the source timestamp by client to process database can be configured in the APROL coupling for the client at connection (session) level. Acceptance can be switched on or off using option "Save SourceTimestamp". In the default setting, the source timestamp is transferred to the process database.
Provision of data	Transfer of the source timestamp by UaRClient to connected OPC UA server can be configured in the APROL coupling for the client at connection (session) level. **Note:** **Not all OPC UA servers support the acceptance of a source timestamp and may reject a set source timestamp with error "BadWriteNotSupported" and refuse to accept the changed value.** **The server timestamp is currently neither evaluated by UaRServer nor UaRClient. With the UaRServer, the server timestamp for provided values in nodes is set to the time of acceptance of the value from the process database.** In the default setting, option "Write source timestamp" in the coupling at connection level (session) is set to "automatic". The client then automatically determines whether a server accepts a source timestamp. If a source timestamp is received, a source timestamp is transferred in the context of the session for each further time that a value is written. Otherwise, no source timestamp is transferred for each further write procedure. Alternatively, writing the source timestamp in the coupling can be permanently switched off or on. If writing is switched on, the report of the OPC UA runtime client should always be checked for errors when writing values.

Table 2: UaRClient



Context: OPC UA Runtime Client Configuration | **OpcUaClientConfiguration** | Connection configuration | **Session01**

Relevance:

Connections (CC)

- ○ Device-Free Connection
- ⊕ ● BuR Gateway Connection (2)
- ⊕ ● Compatibility Connection (1)
- ⊕ ● PDA (1)
- ○ FMS
- ○ HPC
- ○ Simatic S5/S7
- ⊕ ● APROL MQTT Client Configuration (1)
- ⊖ ● OPC UA Runtime Client Configuration (1)
  - ⊖ OpcUaClientConfiguration
    - ⊕ ● Derived data types (1)
    - ⊕ Runtime
    - ⊖ Session01
      - ○ Derived data types
      - ⊕ Parameters
      - ⊖ ● Subscriptions (1)
        - ⊕ Subscr01
      - Methods
- ⊕ ● OPC UA Runtime Server Configuration (1)
- ⊕ ● OPC (1)
- ○ 3964R
- ⊕ ● Dispatcher (1)
- ○ Event Driver
- ○ RK512
- ⊕ ● SysDataTransfer (1)

Session name	!	Session01
URL Server 1	!	opc.tcp://192.168.172.13:4840
Redundancy mode		None
URL Server 2		
Redundancy failover timeout		5000
Node monitoring		Monitoring
Write SourceTimestamp		Automatic
Store SourceTimestamp		
Security mode		
Security policy		None
User name		OpcUaSystemOperator
Password		••••••••
Password validation		••••••••
Default OPC UA node identifier type		String
Default OPC UA node namespace		urn:B&R/pv/
Default OPC UA datatype node identifier type		Numeric
Default OPC UA datatype node namespace		http://opcfoundation.org/UA/
Default queue size		1
Default queue overflow		Discard oldest
Description		049: Controller - Tank

Figure 12: Receiving and writing the source timestamp

3 APROL R4.2-01 release notes

3.1 Central access to certificates for configuration of OPC UA 3rd-party applications

After the configuration of your own applications in the common certificate store and assignment of certificates/applications in the PKI, the communication partners must be configured.

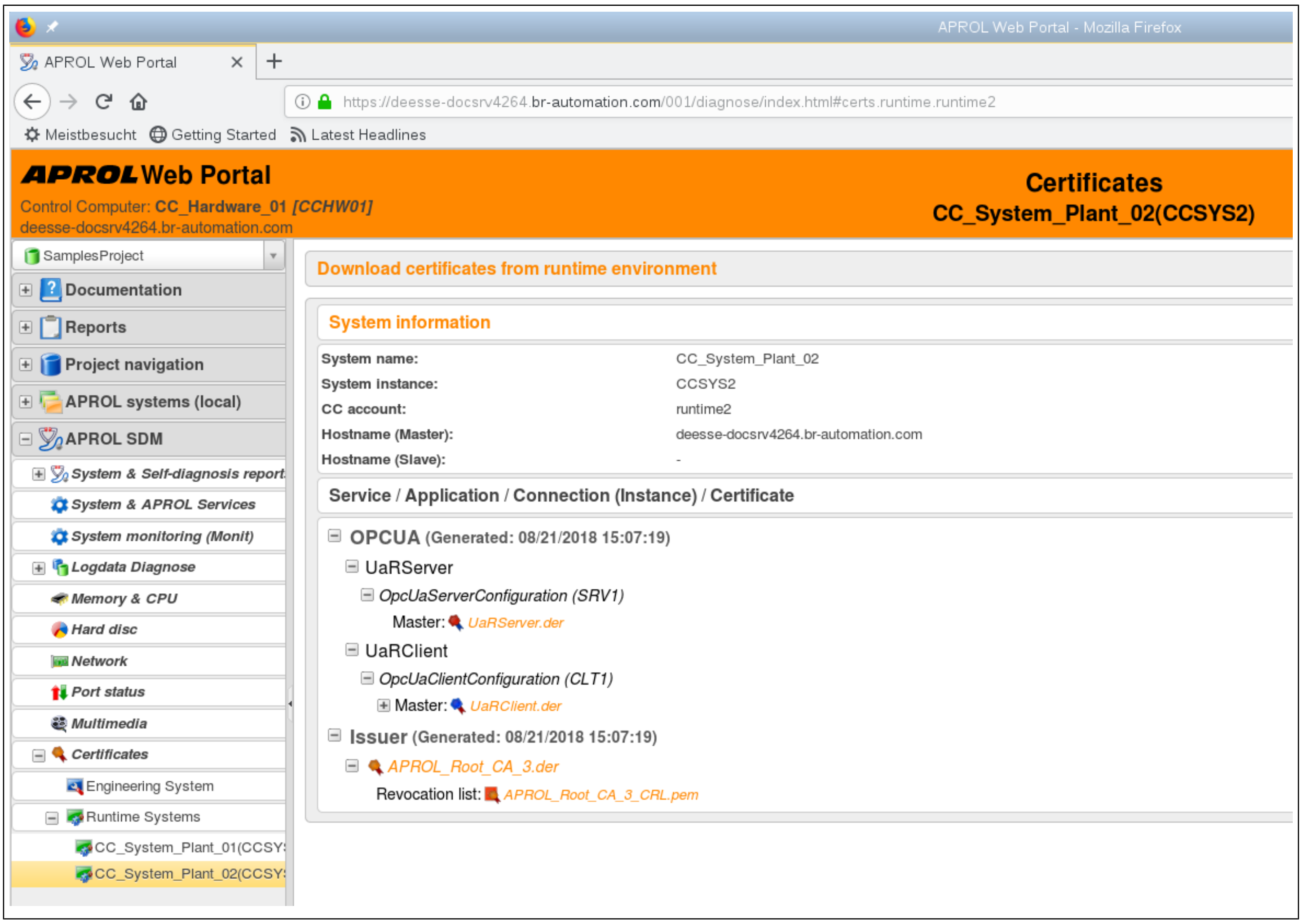
To ensure that the configuration of OPC UA 3rd-party applications can be carried out efficiently and conveniently, the application instance certificates are offered for download in the APROL web portal and thus in a central location.

In section "APROL SDM / Certificates" of the APROL web portal, you can download the application instance certificates and associated issuer certificates (root certificates) of the partner including the associated certificate revocation list (if available):

- Via selective access to a runtime server (activated certificates in the "download status")
- Via access to the engineering server (status after build procedure)

Advantages of accessing the engineering server:

- If engineering is continued, the future active download state can be downloaded.
- Configuration of the OPC UA 3rd-party applications can be performed BEFORE the download, so that communication can start directly after the download is completed.



Certificates
CC_System_Plant_02(CCSYS2)

Download certificates from runtime environment

System information

System name:	CC_System_Plant_02
System instance:	CCSYS2
CC account:	runtime2
Hostname (Master):	deesse-docsrv4264.br-automation.com
Hostname (Slave):	-

Service / Application / Connection (Instance) / Certificate

```
⊟ OPCUA (Generated: 08/21/2018 15:07:19)
   ⊟ UaRServer
      ⊟ OpcUaServerConfiguration (SRV1)
           Master: UaRServer.der
   ⊟ UaRClient
      ⊟ OpcUaClientConfiguration (CLT1)
         ⊞ Master: UaRClient.der
⊟ Issuer (Generated: 08/21/2018 15:07:19)
   ⊟ APROL_Root_CA_3.der
        Revocation list: APROL_Root_CA_3_CRL.pem
```

Figure 13: Convenient distribution of certificates for APROL OPC UA applications via download in the APROL web portal

> **Note:**
>
> **"Build (project)" is required to display the certificates in the APROL SDM.**

> **Information:**
>
> **For detailed information, see chapter "OPC UA in APROL" of manual "F1 - Drivers for B&R couplings".**

3.2 Extensions to MQTT in APROL

Usage of MQTT has been extended in the current APROL release with the following functionalities:

> **Information:**
>
> **For detailed information, see chapter "MQTT in APROL" of manual "F1 - Drivers for B&R couplings".**

Storage of APROL metadata on the MQTT server

A fixed set of APROL metadata can be sent for the analysis tools "behind" the MQTT server (e.g. the database tools of the cloud). This metadata encompasses static information **that does not change during the existing connection and is therefore transferred directly after the connection is established**.

Init data for publish blocks

AprolMqttClient supports transfer of init data, i.e. data that is transferred **once to the server after each connection is establishedand before the telemetry data transfer of the block is performed**.

This inti data can be configured in the context of the separate tab "Init payload", whereby substitution of different pin attributes and block data can be used. The use of init data is optional.

Since data is only transferred once, static data such as block information, pin data types, etc. can be transmitted here.

Storage of "Stream analytics" data for query in APROL SDM

Under the tab "Stream analytics", any data can be stored by the user and downloaded to the runtime system. For example, SAQL statements for further processing of publish messages can be stored centrally so that they are then available in the cloud for input in the analysis tool.

SQL statements for creating SQL table structures in the cloud

To process the data of the publish block in the Azure Cloud, it must first be temporarily stored in an SQL database. For data sets consisting of the complete pin layout of all input pins, the SQL statement for generating the SQL tables can be generated under tab "DDL" using checkbox "Automatically generate table definitions from pins".

For your own data or for another environment, this automatic generation can be replaced by manual entry (if the checkbox is not enabled). This stored data is also downloaded to the runtime system and can be opened from any location via the APROL SDM.

3.3 Extension of CAE libraries

CAE library "Core"

An additional CAE library "CORE" offering technology functions is delivered as standard in APROL R4.0-13 and later. These may be functions that already exist in AS libraries (e.g. Mechatronic libraries).

The following blocks have been added to this library:

- MTDataStatistics01 (detection of elementary statistical data such as mean value, standard deviation, etc. from a signal)
- MTLookUpTable2D01 (any two-dimensional function f(x,y) using interpolation points)
- MTPredictTripleExpSmooth01 (prognosis of time series with linear trend and seasonal effects)
- MTProcessSteadyState01 (identification of the steadiness of a signal)

CAE library "SysMon"

Color dynamics have been assigned to all objects of all graphic blocks. This makes it possible to adapt the appearance of a CAE library to specific projects.

> **Note:**
>
> **Fonts, colors and images of libraries can be redefined in the CAE project properties.**

4 APROL R4.2 release notes

4.1 K Desktop Environment (KDE)

Changeover to KDE Plasma 5

The desktop environment was changed to "KDE Plasma 5".

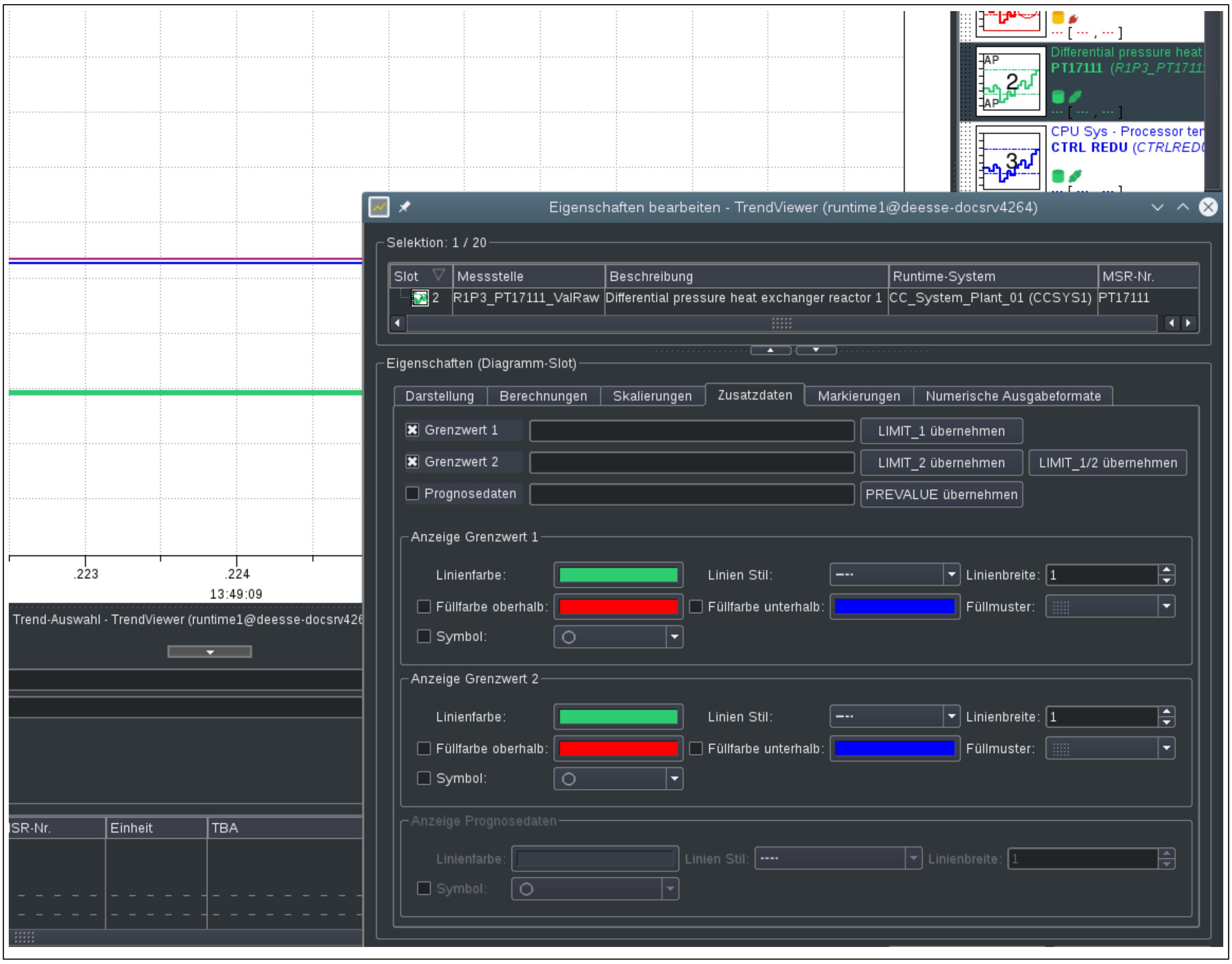
> **Note:**
>
> **Desktop environment "KDE Plasma 5" has been adapted to APROL's requirements and allows a simple and error-free operation of the APROL system software.**

Switching the APROL style

Beside the familiar, classic look & feel of APROL front ends and desktops (classic style), APROL can also be switched to a "Dark style" in R4.2 and later.

"Dark style" displays front ends and desktops in a dark design with light font and icons with reduced color palette (mainly from the *Google Material Design*).

Switching is carried out in the CC account (engineering / runtime / operator system) via KDE menu option "**System configuration / APROL style**".



Eigenschaften bearbeiten - TrendViewer (runtime1@deesse-docsrv4264)

Selektion: 1 / 20

Slot	Messstelle	Beschreibung	Runtime-System	MSR-Nr.
2	R1P3_PT17111_ValRaw	Differential pressure heat exchanger reactor 1	CC_System_Plant_01 (CCSYS1)	PT17111

Eigenschaften (Diagramm-Slot)

Darstellung | Berechnungen | Skalierungen | Zusatzdaten | Markierungen | Numerische Ausgabeformate

☒ Grenzwert 1 — LIMIT_1 übernehmen

☒ Grenzwert 2 — LIMIT_2 übernehmen — LIMIT_1/2 übernehmen

☐ Prognosedaten — PREVALUE übernehmen

Anzeige Grenzwert 1

Linienfarbe: 🟩 Linien Stil: --- Linienbreite: 1

☐ Füllfarbe oberhalb: 🟥 ☐ Füllfarbe unterhalb: 🟦 Füllmuster:

☐ Symbol: ○

Anzeige Grenzwert 2

Linienfarbe: 🟩 Linien Stil: --- Linienbreite: 1

☐ Füllfarbe oberhalb: 🟥 ☐ Füllfarbe unterhalb: 🟦 Füllmuster:

☐ Symbol: ○

Anzeige Prognosedaten

Linienfarbe: Linien Stil: ---- Linienbreite: 1

☐ Symbol: ○

Figure 14: TrendViewer in "Dark style"

4.2 Secure Boot: Securing the boot procedure against unnoticed changes

> **Information:**
>
> **For detailed information (including requirements for using Secure Boot), see chapter "Secure Boot" of manual "A2 - Getting started".**

On a server with UEFI-compatible firmware, Secure Boot can be used to protect the boot procedure against unnoticed changes.

Secure Boot allows you to detect changes to the boot procedure and prevents programs from untrusted sources from starting. The spread of malware attached to the boot procedure can thus be detected and prevented.

Using certificates stored in the firmware, only a signed bootloader can be executed during the boot procedure. This bootloader also only executes signed programs.

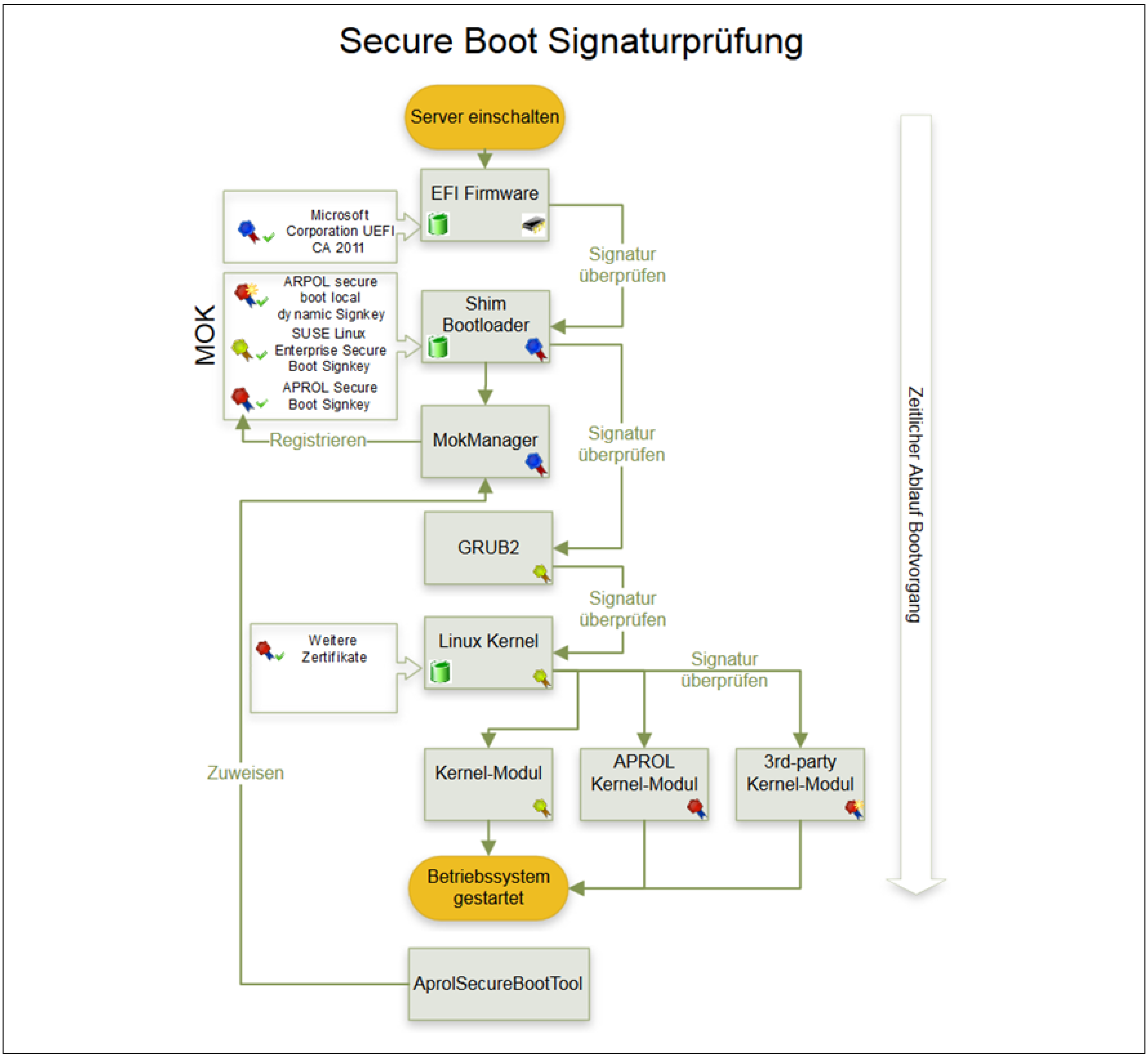


Figure 15: Diagram for using signatures for Secure Boot

4.3 Advanced Intrusion Detection Environment - AIDE

Information:

For detailed information, see chapter "'Advanced Intrusion Detection Environment - AIDE" of manual "A2 - Getting started".

The AIDE framework makes it possible to identify unwanted changes to files and folders. The supplied **A**dvanced **I**ntrusion **D**etection **E**nvironment framework is used to monitor directory */opt/aprol*.

As Linux superuser "root", a manual file system scan (via KDE menu option "Diagnostics") can be started on the basis of the supplied example configuration.

Note:

The example configuration that is also supplied is intended to assist the system administrator in creating an individual and comprehensive AIDE configuration.

After the scan procedure is completed, an associated report with the detected results is displayed. The report can be opened at any time in the APROL SDM.

> **Note:**
>
> **The AIDE database is updated after each APROL installation.**

4.4 Forwarding relevant process data via MQTT client

> **Information:**
>
> **For detailed information, see chapter "MQTT in APROL" of manual "F1 - Drivers for B&R couplings".**

An MQTT client is available for forwarding relevant process data and in addition to direct communication with an MQTT broker (MQTT server), it can also establish communication with the cloud (currently *MS Azure Cloud*) and pass on data.

> **Note:**
>
> ***MQTT* is an open messaging protocol for machine-to-machine communication (M2M), i.e. to transfer telemetry data in the form of messages between suitable terminal devices (e.g. actuators and sensors).**

The process data to be forwarded to the cloud or to the MQTT-Broker is selected using a predefined coupling type in the context of project part "APROL system".

> **Note:**
>
> **The AprolMqttClient is therefore provider for all project variables defined in the context of this configuration.**

The new MQTT publishing block can be used for the convenient composition of process data so that the data can be configured directly where it arises (thus also in hyper macros) for recording and transport with MQTT.

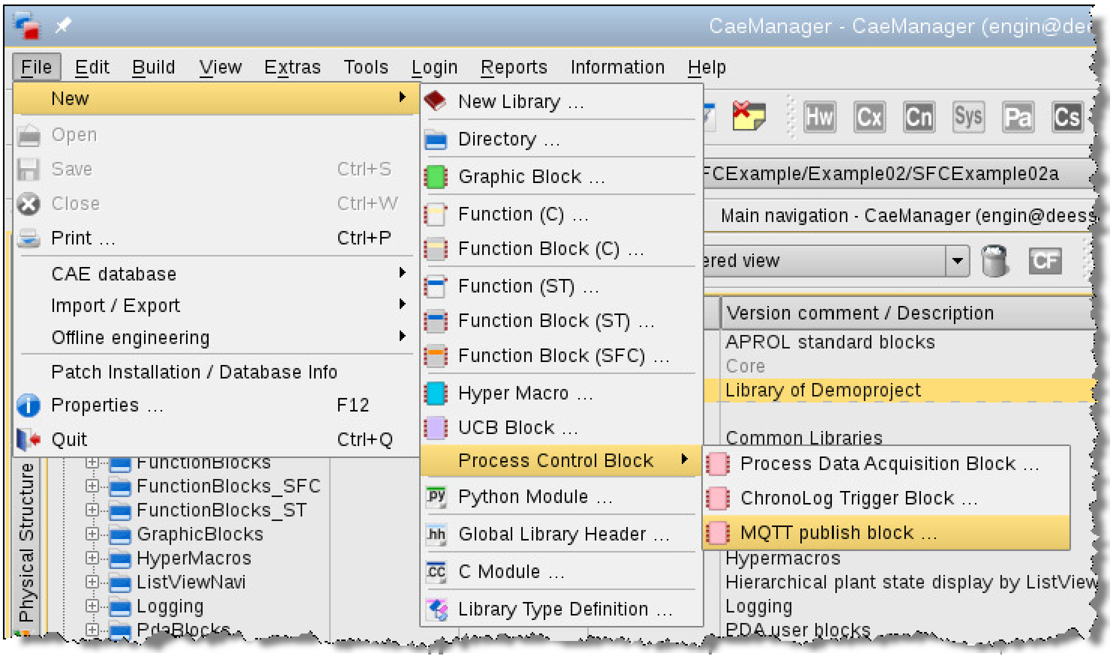


Figure 16: New MQTT publishing block

4.5 Open standardized and vendor-independent communication via OPC UA

> **Information:**
>
> **For detailed information, see chapter "OPC UA in APROL" of manual "F1 - Drivers for B&R couplings".**

Both applications "OPC UA runtime server" and "OPC UA runtime client" are available on the APROL runtime server for open, standardized and vendor-independent communication. Couplings for connecting a client to a server are created here and thus make certain nodes available as process variables in the system.

> **Note:**
>
> **The OPC Unified Architecture (OPC UA) communication protocol is based on the client-server principle and allows seamless communication of individual sensors and actuators up to the ERP system.**

The CaeManager creates a simple configuration of the OPC UA runtime server and OPC UA runtime client using ready-made APROL couplings.

In addition, configuration of the OPC UA server variables of a B&R controller is already possible directly from project part "Controller" starting with APROL R4.0-12.

4.6 Online parameter management

> **Information:**
>
> **For detailed information, see chapter "Online parameter management" of manual "D1 - System manual".**

APROL projects can be commissioned much more effectively and conveniently by using online parameter management.

The new operation dialog boxes of the online parameter management allow the following:

- Comparison and compensation of parameters of several units (hyper macros), e.g. of motors, dosing feeders, valves
- Transferring parameters from one unit to another (selective export/import in runtime)
- Feeding parameters back to the CAE environment after optimizing the plant

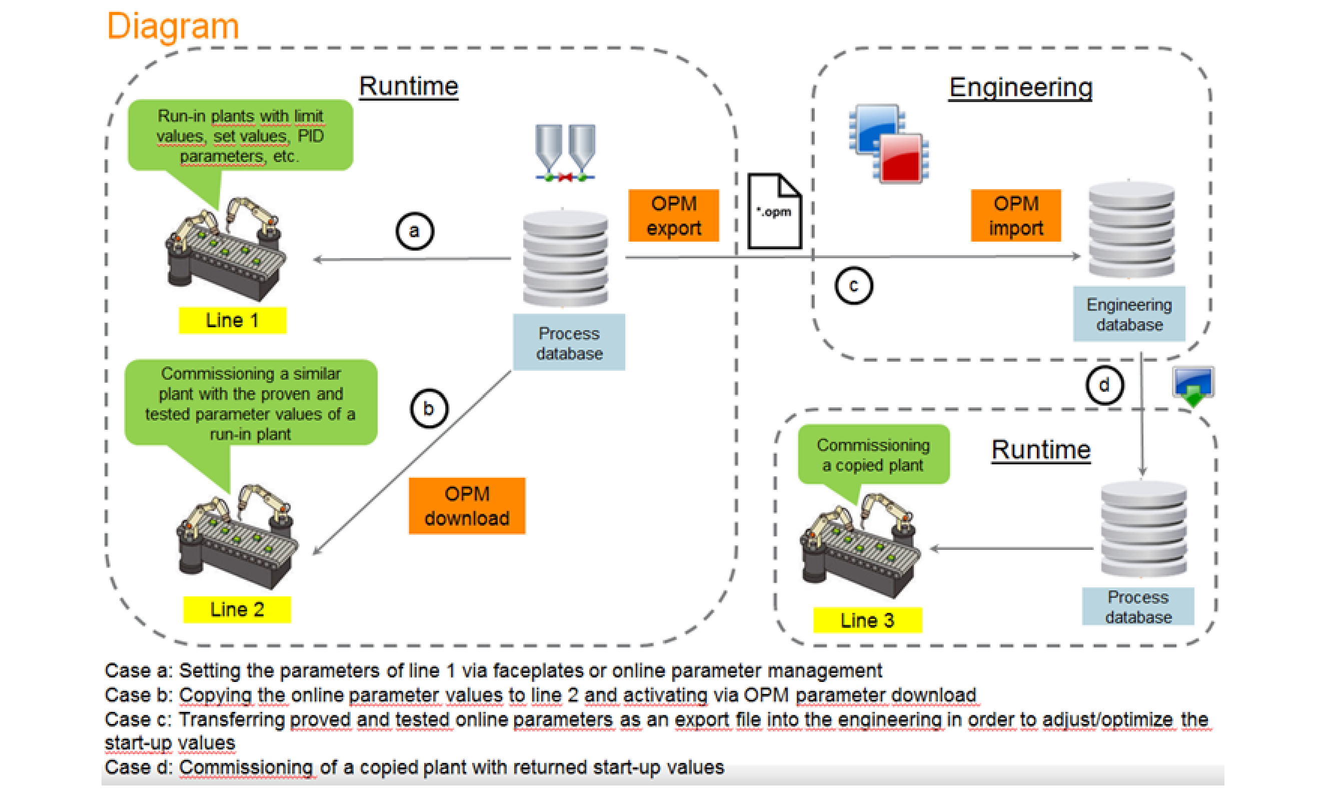


Diagram
Runtime
Run-in plants with limit values, set values, PID parameters, etc.
Line 1
a
Process database
OPM export
*.opm
Engineering
OPM import
Engineering database
c
Commissioning a similar plant with the proven and tested parameter values of a run-in plant
b
OPM download
Line 2
d
Commissioning a copied plant
Runtime
Line 3
Process database

Case a: Setting the parameters of line 1 via faceplates or online parameter management

Case b: Copying the online parameter values to line 2 and activating via OPM parameter download

Case c: Transferring proved and tested online parameters as an export file into the engineering in order to adjust/optimize the start-up values

Case d: Commissioning of a copied plant with returned start-up values

Figure 17: Possible workflows in practice

Summarized, online parameter management offers the following advantages:

- Simple commissioning
- Clear display of online parameters
- Convenient application of online parameters via drag-and-drop

4.7 Negation on block pins and CFC and hyper macro border entries

Information:

For detailed information, see chapter Negation of block pins and CFC / Hyper macro entries of manual "B2 - Project engineering".

Negation can be set interactively on input and output pins of block instances in a CFC or hyper macro as well as on the border entries of a CFC or hyper macro.

Negation can be configured via shortcut menu option "Negation" of a block pin / border entry of type BOOL.

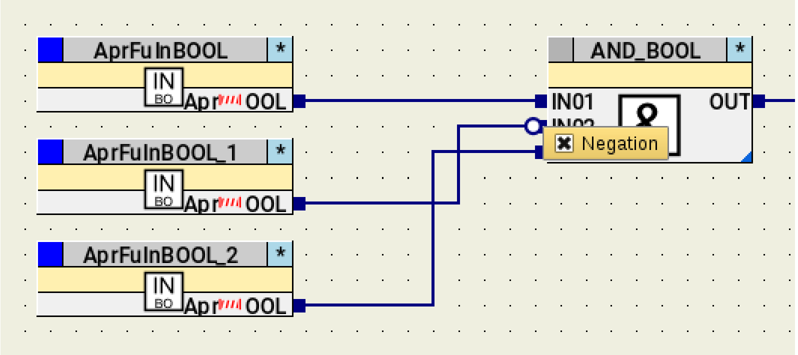


Figure 18: Configuration of the negation on the block pin

This makes it possible to invert a Boolean signal in the CFC / hyper macro logic and use this negated value for further processing of the CFC or hyper macro.

The configured negations are passed on to the destination of the connection and applied there.

4.8 Dependency check for engineering (requirement management)

> **Information:**
>
> **For detailed information, see chapter "Dependency check for engineering (requirement management)" of manual "B2 - Project engineering".**

Creating a CAE project with APROL can usually be performed without strictly adhering to a fixed order of events.

Nevertheless, there are dependencies between respective project parts that especially concern the build procedure, for which the APROL system enters notes about required actions (requirements) in the context of the dependent project parts.

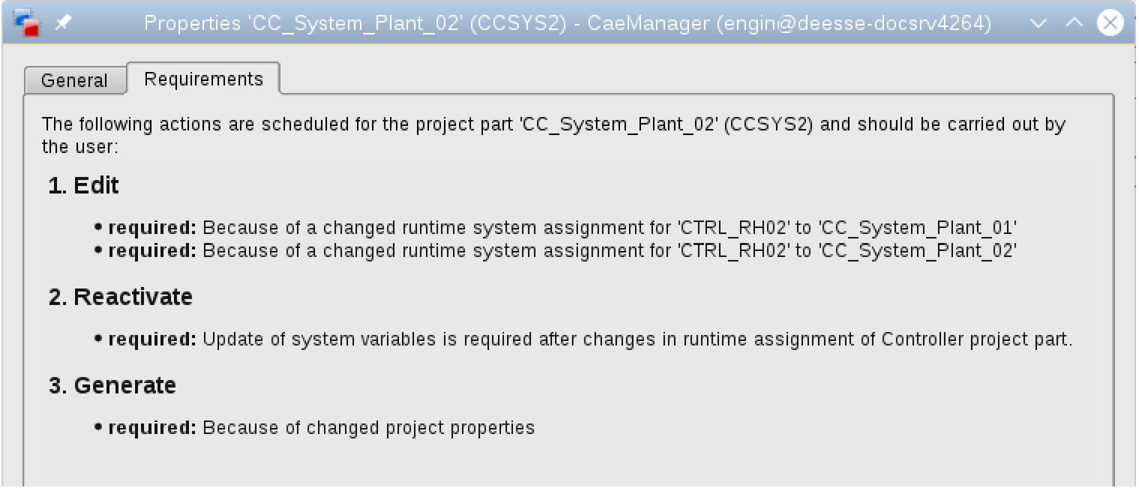
> **Note:**
>
> **This has significantly increased the transparency of the APROL system software.**

The APROL functionality for detecting and marking dependencies (requirements management) determines dependencies for actions such as editing, saving and activating and enters these requirements in the relevant project parts.

The affected project parts are marked with different icons so that the necessary actions are clearly displayed to the user. These actions can then be performed manually by the user.

The requirements (dependencies) for the respective project part are displayed in the following places:

- Tooltip of the project part (display of the most high-order action)
- Properties dialog box of the project parts (in a separate tab)
- When opening a project part, a message dialog box is displayed if CAE messages and/ or actions derived from the requirements exist for this project part.



Properties 'CC_System_Plant_02' (CCSYS2) - CaeManager (engin@deesse-docsrv4264)
General
Requirements

The following actions are scheduled for the project part 'CC_System_Plant_02' (CCSYS2) and should be carried out by the user:

1. Edit
   - **required:** Because of a changed runtime system assignment for 'CTRL_RH02' to 'CC_System_Plant_01'
   - **required:** Because of a changed runtime system assignment for 'CTRL_RH02' to 'CC_System_Plant_02'
2. Reactivate
   - **required:** Update of system variables is required after changes in runtime assignment of Controller project part.
3. Generate
   - **required:** Because of changed project properties

Figure 19: Separate tab in properties dialog box of the project part

4.9 Extension of CAE library "SysMon"

> **Information:**
>
> **For information about new features in APROL CAE libraries, see chapter "Scope of the APROL Libraries" of manual "B3 - CAE library engineering".**

There are the following corrections and updates in CAE library "SysMon":

- Provision of many new blocks for APROL system monitoring (**including** monitoring of controller including base rack / display and monitoring of APROL systems (runtime, operator, gateway)
- Many new functions and monitoring (**including** monitoring OPC UA servers and clients on the control computer)

4.10 Extended diagnostic options for the ANSL server

ANSL server diagnostics provides comprehensive ANSL connection diagnostics of all incoming connections to the controller's ANSL server so that all objects of all connected clients, i.e. all connected control computers and controllers connected via cross-communication, can be diagnosed.

All ANSL connection information of the controller and all registered event PVs are available via an ANSL service.

This is the following data of the respective client, for example:

- Connection data (IP addresses, hostnames, etc.)
- ANSL connection parameters
- Number of ANSL objects
- Transfer rate in bytes/s
- Event rates for ANSL requests and responses
- Number of event PVs
- Change rate of event PVs

The new dialog box can be opened from the following places:

- ControllerManager: Via shortcut menu option "ANSL server diagnostics" of the connected controller or via associated toolbar button
- CaeManager: Via shortcut menu option "Controller diagnostics / ANSL server diagnostics" of a controller or via main menu option "Tools / Controller diagnostics / ANSL server diagnostics"
- DownloadManager: Via shortcut menu option "Controller diagnostics / ANSL server diagnostics" of a controller

4.11 Optimizations in CAE management

Switchable tooltips for project parts

In the user options (tab "Productivity"), the tooltips for project parts in the CaeManager navigation can be switched off. The tooltips can be disabled either for tab "Context structure" or for all tabs (i.e. all navigation views).

Note:

Switching off tooltips in the Context Structure can significantly reduce the processor load in very extensive CAE projects and thus helps work more smoothly, especially in concurrent engineering.

Alternatively, tooltips can be disabled via associated toolbar button.

Restructuring of menus and shortcut menus in the CaeManager

The menus and shortcut menus in the CaeManager have been restructured according to the following aspects:

- All functionalities provided in the application are now also available via the menu bar.
- The grouping of the entries in the shortcut menu corresponds to the grouping in the toolbar.
- Actions that cannot be used in the current context are grayed out. The reason why a menu option cannot be operated is displayed in the status bar.

Extended operating options of CAE navigation

The columns of the CAE navigation can now be moved and shown or hidden. The changes here are saved user-specifically and restored when the application is restarted.

The context page of a process graphic was extended with a preview view. Using a separate toolbar, the preview images can be enlarged or reduced.

Starting directory for loading project parts

To reduce the loading time of the Context Structure of a process graphic, the project content to be loaded can be limited.

This is possible by only loading the CFCs starting with the specified path depth when the Context Structure is opened.

A path depth can be specified in the user options that can be temporarily reduced in the Context Structure using a button.

Extending the project properties with the domain name

The specification of a default domain name can be entered globally in the project properties in APROL R4.2 and later.

In all of the different places where a domain name is used, this can now be conveniently applied from the project properties or manually overwritten.

The specification for the domain name in the project properties (if it exists) can be applied via the shortcut menu in the control computer.

4.12 Extensions in the APROL HMI

New visualization element "Spider chart"

The APROL HMI has been extended by widget "Spider chart", which can display up to 16 channels with a maximum of 3 values each for displaying process data in a spider chart.

> **Note:**
>
> **Therefore, values of different process data and their relation to each other can be clearly and easily displayed.**

By configuring minimum and maximum tolerable limit values per channel and an suitable automatic scaling, the permissible values are displayed in a defined ring of the spider chart widget so that overshooting or undershooting the permissible values can easily be visually detected by leaving the ring.

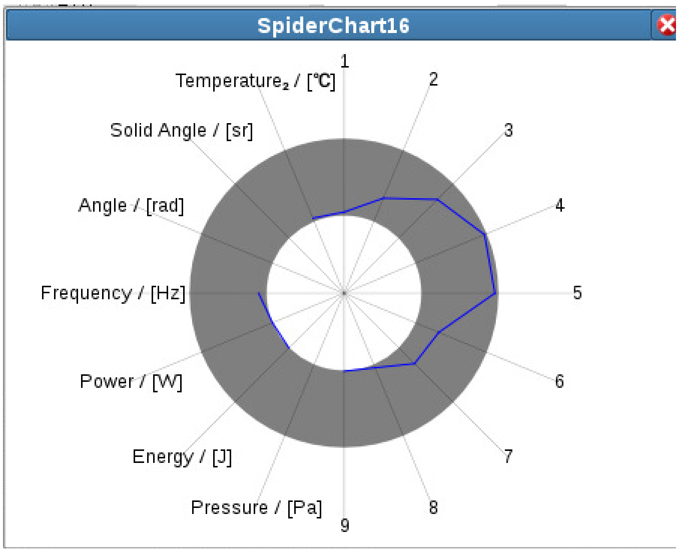


Figure 20: New visualization element "Spider chart"

Examples of the numerous configuration settings:

- Dynamic hiding of individual axes (the resulting display after hiding individual axes can be set with this)
- Additional polygons (caused by configuring additional values per channel) can be shown and hidden dynamically.

> **Note:**
>
> **Scalable graphic blocks named "SpiderChart" are available as an example in group "AnalogValues", in CAE library "PB_Bas" and can be used directly in an APROL project.**

Additional extensions in the APROL HMI

In addition, the APROL HMI has been extended with the following convenient functions:

- Standard way of aligning text on buttons
- Displaying images in user-defined tooltips
- Filter functionality for the selection in combo boxes

4.12.1 Visualization element for displaying video files or video streams

The APROL HMI was extended with a new visualization element that supports displaying video files and/or video streams in the normal formats.

Brief detailed information:

- The video player to be used is selected with input "VideoPlayer". Video players "mplayer" and "vlc" are currently supported. "vlc" will be used by default if no player is selected.
- The name of the video file that must exist in directory */home/<Runtime system>/RUNTIME/VIDEO* is passed to block input "FileOrURL".

As an alternative to the video file, a URL for a stream can be specified. The supported formats depend on the player used and the installed codecs.

> **Important!**
>
> **"mplayer", "vlc" and codecs are not supplied together with APROL due to licensing reasons. "mplayer" and "vlc" can be installed afterwards.**
>
> **Please note the respective legal situation in your country before starting installation.**

> **Note:**
>
> **Block "MediaPlayer" is available in B&R library "PB_Bas" (group "Functions"), uses the new visualizations element as an example and can be used to display video streams.**

4.13 Secure Remote Maintenance (SiteManager)

> **Information:**
>
> **For detailed information (including installation and configuration), see chapter "Remote maintenance with SiteManager Embedded for Linux" of manual "A2 - Getting started".**

SiteManager Embedded for Linux is supplied together with APROL and allows a high-speed, simple and secure remote access over the Internet or private WAN.

4.14 CSV export of web reports

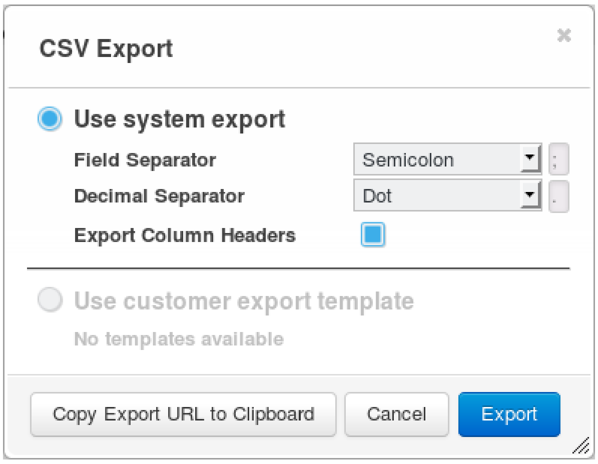
> **Information:**
>
> **For detailed information, see chapter "CSV export for web reports" of manual "B2 - Project engineering".**

CSV export is available for all web reports so that the content of APROL reports can be supplied in a suitable form for further processing by programs from 3rd-party suppliers (*Excel, LibreOffice,* etc.).

The configuration of separators for columns and fields, separators for decimal numbers and the option to hide columns make import and further processing much simpler.

The filtering and sorting set in the report and the table layout selected by the customer are taken into account.

The CSV export is comfortably configured in a separate dialog box.



CSV Export

● Use system export

Field Separator: Semicolon ;

Decimal Separator: Dot .

Export Column Headers ☑

○ Use customer export template

No templates available

Figure 21: Configuration of the CSV export

5 Revision history

Manual version	**Date**	**Change**	**Author** ***Reviewed by***
7.10	2019-01-18	Chapter "APROL R4.2-05 release notes": Created.	KSc *HSc*
7.05	2018-04-17	New chapter "Validation of the B&R Automation PC 910 and 3100 with Trusted Platform Module".	KSc *SG*
7.04	2018-03-28	New chapter "APROL R4.2-03 release notes".	KSc
7.03	2018-02-28	Manual: Updated with formal adjustments.	KSc
7.02	2018-01-12	New chapter "APROL R4.2-01 release notes".	KSc
7.01	2017-11-21	New chapter "APROL R4.2 release notes".	KSc

Table 3: Revision history

6 Figure index

7 Table index