APROL R 4.2 – Industrial Control System

Roadmap und Neuerungen des Build 06

APROL R4.2 – Industrial Control System

Roadmap

APROL R4.2 – Industrial Control System

Innovation with Continuity

Life cycle phase

Active
- Product marketed
- Available for sale for new installations
- Supported

Classic
- Functional replacement available
- Available for sale for expansions
- Supported

Limited
- New product no longer manufactured
- Supported - with best practical effort

Obsolete
- No longer available for sale or delivery
- Support not available

Customer commitment

B&R's life cycle management policy states that *no product will be removed from active sale until a compatible, equivalent or superior product is available.*
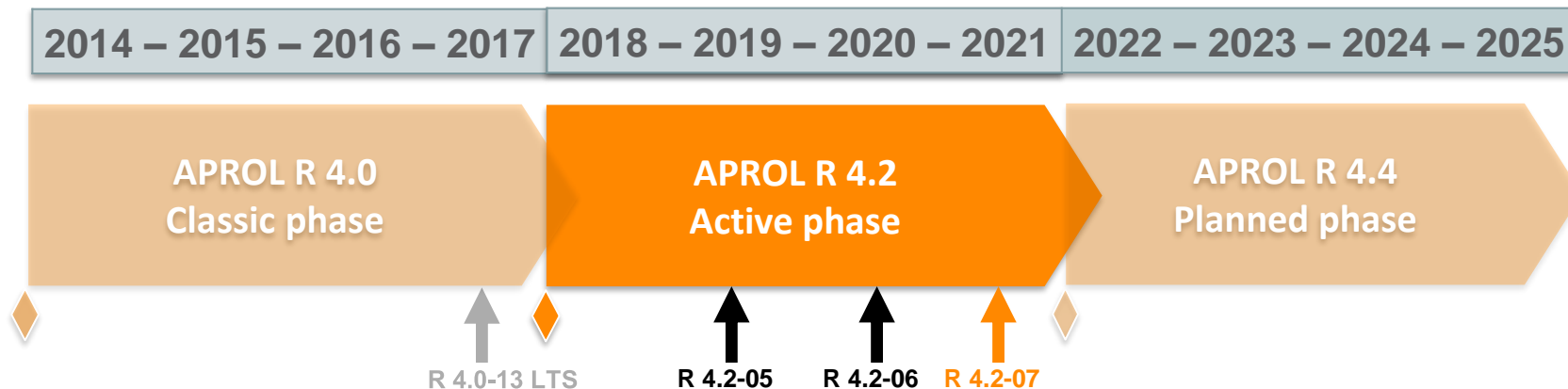
The strategy of functional upward compatibility assures the control application can be carried forward to a new hardware platform.

APROL is designed to facilitate the adoption of new technology with continuity of the underlying customer applications

- Always a path forward
- Protection of intellectual assets
- Underlying products are sustained by defined and documented lifecycle phases
- Active until functional equivalent available

APROL R4.2 – Industrial Control System

Releases and builds

2014 – 2015 – 2016 – 2017	2018 – 2019 – 2020 – 2021	2022 – 2023 – 2024 – 2025

APROL R 4.0
Classic phase

APROL R 4.2
Active phase

APROL R 4.4
Planned phase

R 4.0-13 LTS

R 4.2-05   R 4.2-06   R 4.2-07

Build 06

Focus on System hardening & security improvements Phase 1
1600+ Improvements & closed tickets
* 800+ System extensions*

Build 07

Focus on asset management & security improvements Phase 2

APROL R4.2 – Industrial Control System
Build 06   Major Features

Build 06 – Security Improvements
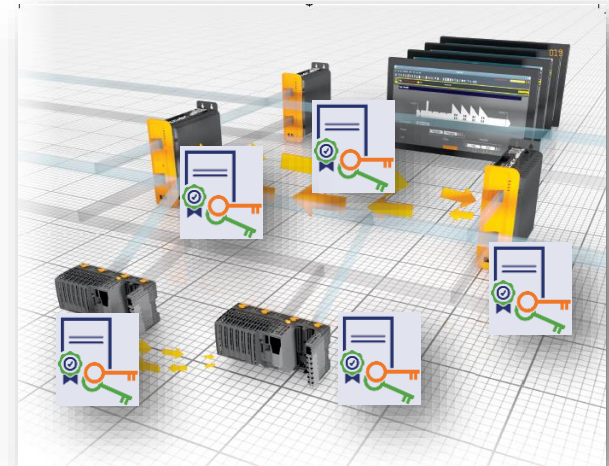
Usage of CA-signed Certificates
Instead of using a self-signed Certificate,
the usage of CA-signed certifiactes on
any secure communication is now possible

Certificate based Encryption
System communication can be fully encrypted
(e.g. PLC, Webserver, Remote access)

Best in class PKI Configuration Wizard for any secure communication
Enables engineers to configure a secure communication and helps to identify
upcoming certificate issues

Build 06 – Security Improvements

Firewall and white list handling for Controller communication
The firewall is used to restrict network access based on identification of sender or receiver and based on services or port rules. Project rules are applied automatically, additional rules can set on each controller.

Removement of default system user & password
*Default username and password can be high security risk.
To meet security guidlines, default APROL users and passwords are removed and now part of project configuration*

Advanced Intrusion Detection Enviroment
Protect system configuration against unattended changes

Build 06 – New Authentication Server

New authentication server „389 Directory Server"
replaces openLDAP server.

Authentication server
for Operator, mappView, OPC-Ua

Decentralized deployment
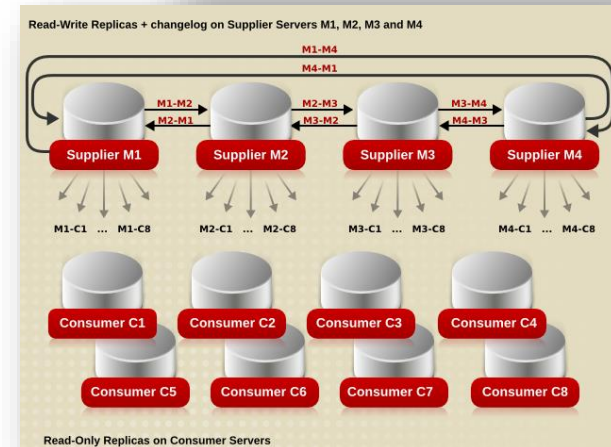*each MultiRuntimeServer can host an own instance*

Creation of users /operators
direct in 389 Directory Server.

Definition of Groups
and assignment to users / operators.

Password modification
during runtime by operator

APROL R4.2 – Industrial Control System

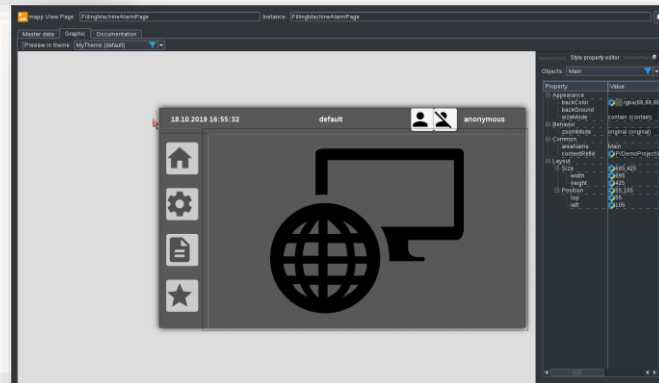**PIN type Grafic reference**
to access graphic blocks across CFC

Reduced project export/import
for onsite commissioning

Encrpyted export/import
CAE content can be encrypted and validated by fingerprint

mappView Editor
Layout-Editor, Content-Editor, Page-Editor

Build 06 – New Hardware

Support for ARsim

Test & Simulate real time environment without hardware controller
Run multiple ARsim on Notebook, PC or Server

NEW X20 Generation X20CPx68x

up to 1.3 GHz Atom CPU
1GB RAM, 1GB Flash on Board
Ethernet Interface for TSN

NEW Highend Generation – X20CP3687X

up to 1.6 GHz Atom CPU
2GB RAM, 2GB Flash on Board
Ethernet Interface for TSN

APC based Controller

APROL supports now configuration of APC as controller

Build 06 – New Hardware features

APC relay module enables binary signal output by operator station

- **APC plug-in module 5AC901.ISIO-00** (Ready-Relay) controlled by ApcHwInfo service.

- **Any wiring carried out via automatically provided system variables.**

- **Startup and shutdown behaviour** predefineable

- **Any states** in the automation logic can be output via Automation PC of the operator station without additional wiring effort.

Industrial Cyber Security – FIDO2 Authentication

YubiKey replaces weak static username/password credentials with strong hardware-backed public/ private-key credentials.

Password less Authentication (FIDO)
Single factor authentication using a hardware authenticator.

Two factor authentication (2FA)
2FA using a hardware authenticator as an extra layer of protection beyond a password.

Industrial Cyber Security – Trusted Platform Module (TPM 2.0)

TPMs are widely used as a root of trust for platform integrity, remote attestation and cryptographic services.

Target Applications
Desktop, Notebook, Tablet, Server, Networking devices.
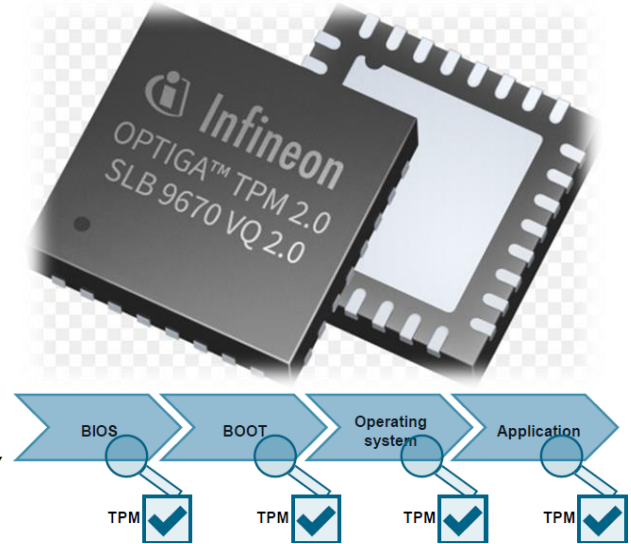
Authentication
Of people and devices so information is exchanged between authorized individuals and devices only.

Encryption
Protects sensitive information by encrypting it and securely storing the secret keys.

Platform Integrity
Check platform, machine and device integrity to identify manipulation.

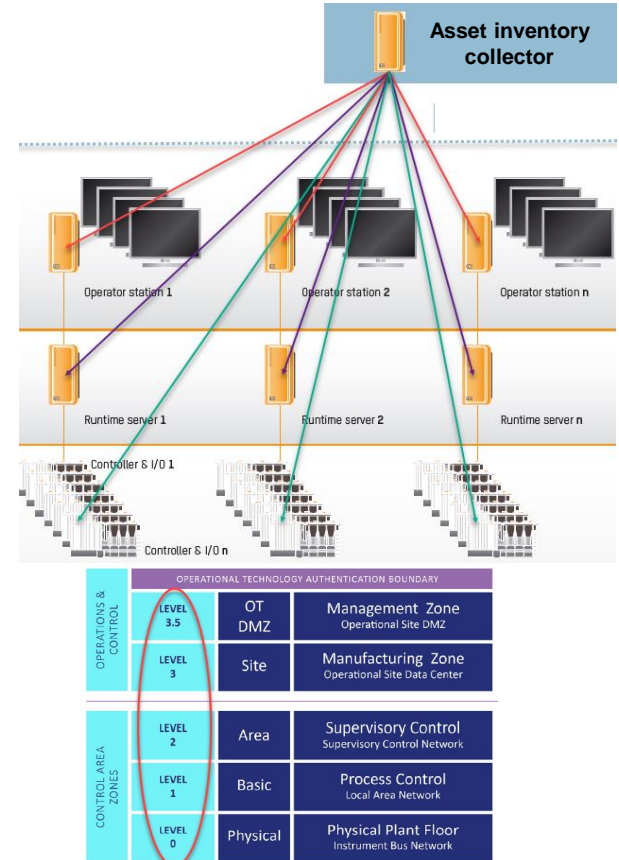# APROL R4.2 – Industrial Control System

Asset Management – OT asset inventory

OT asset inventory is defined as resources (hardware, software, documents, services, people, facilities, etc.) that are of value to an organization and need to be protected from potential risks.

From our point of view it is comprised of **hardware components and software components***.*

Detailed aspects like asset name (project), vendor (B&R), type (CC, CTRL, BC,..), model (X20CP3586,…), serial no., RTOS/GPOS/firmware,
IP/Mac-address, Level 0/1/2/3 (Perdue model) of each asset are included.

System & Self-diagnosis report **"Check installation"**
and **Controller System Diagnostics Manager** *"Upload hardware tree as file (xml)" provides information for unified lists.*

Asset Management – PatchInstaller

New PatchInstaller supports Patch Management of APROL system software and Linux system for all Control Computers.
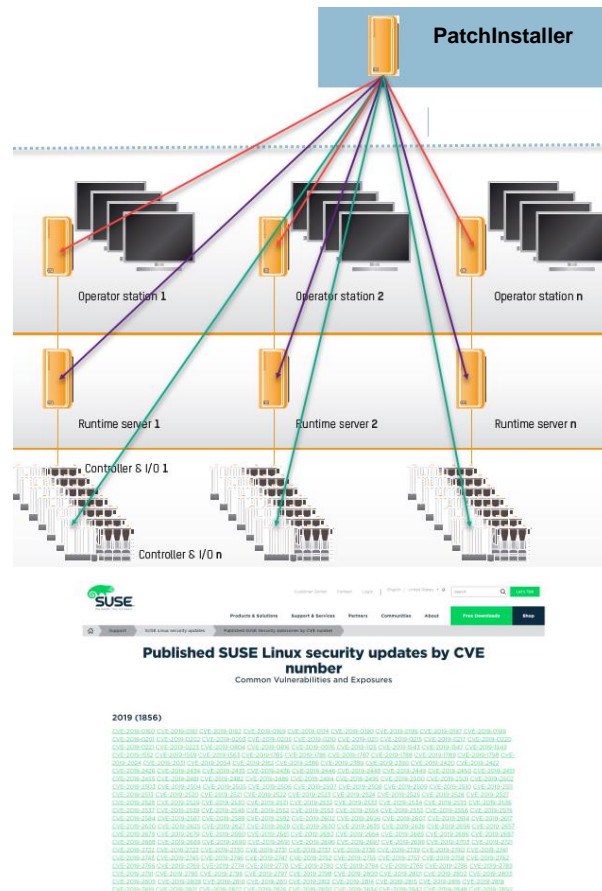
System software and GPOS
Selective and timed installation of patches and AutoYaST updates.

Sequence defineable
Supports grouping of Control Computers (e.q. primary/ secondary, sequence,…).

Update enforcement
Enables confirmed/ unconfirmed update (e.g. unmanned local control centers).

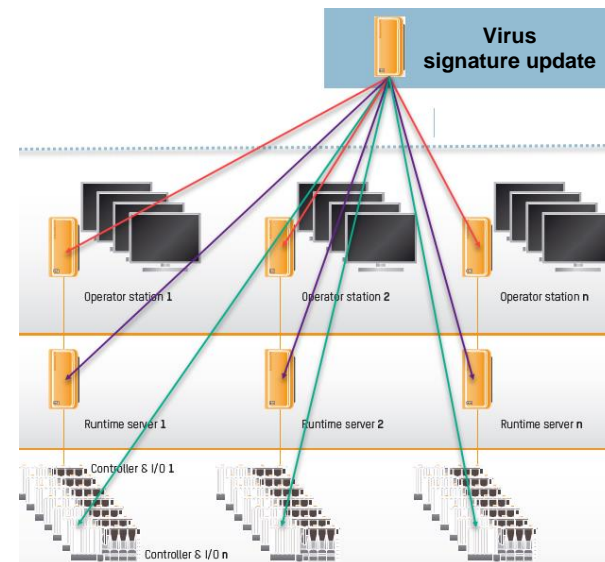## Asset Management – Virus scanner

Virus signature update files are updated on a dedicated station

Local virus scanners
Control computer pulls actualization of virus signatures for local scanner.

Update by update files or updated database
Virus signature database update files.

! Attention: Typical statement (EULA) of virus scanner provider

8. CRITICAL APPLICATIONS. The Software is not fault tolerant and use of the Software is prohibited for on-line control equipment in hazardous environments requiring fail-safe performance, such as the operation of aircraft navigation or aircraft communications systems, air traffic control, life-support systems, human implantation, nuclear facilities or systems, weapons systems, or any other application where failure of the Software could lead to death, personal injury, or severe physical or environmental damage.

Asset Management – Certificate Management
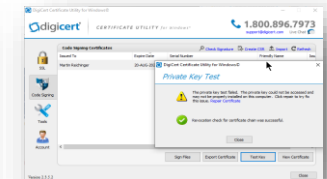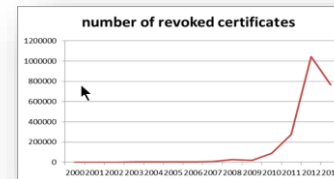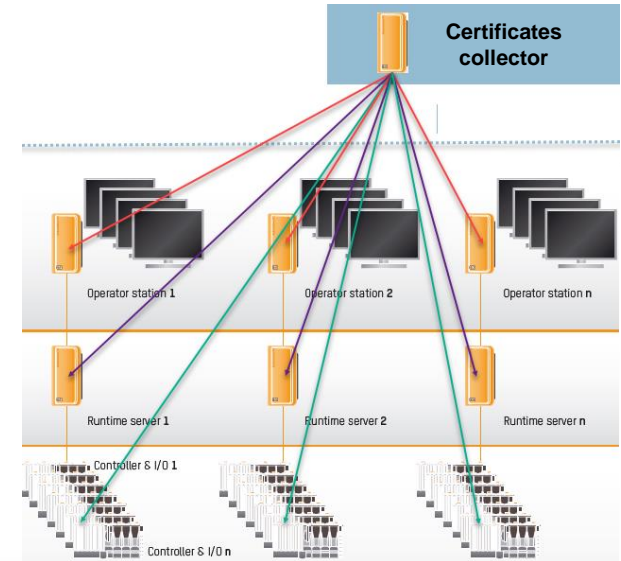
Certificate revocation list (CRL)

*In cryptography, a certificate revocation list (CRL) is a list of digital certificates, that have been revoked by the issuing certificate authority (CA) **before their scheduled expiration date** and should no longer be trusted.*

The number of revoked certificates has increased dramatically in recent years.

The service must collect all certificates whose expiration date has not yet expired.

The URL of the CRL is encoded (crl) in end-entity certificates. The serial number of certificate must be evaluated against revocation list.

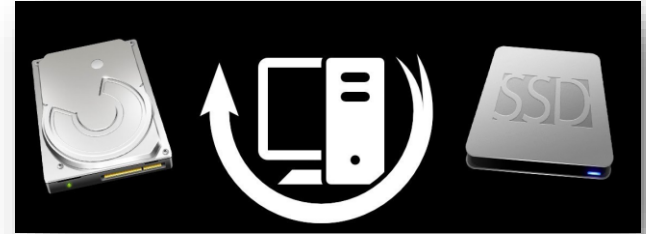*Action: Generate info "n of m revocated certificates"*

APROL R4.2 – Industrial Control System
Tools

Tools – HD Clone

Full Backup & Disaster Recovery Tool
Create Full Backups or fast software recovery after hardware disaster

Delta Backup
Create periodically backups and store only changes

Clone Installation
Fast cloning of drives including changes to disk size or partitioning

Full Validation and Reporting
Each Backup or Restore is validated and finally reports are stored as PDF

Live Präsentation

PERFECTION IN AUTOMATION