DEMAS
DEVICE MANAGEMENT SYSTEM

RITTER
TECHNOLOGIE

INDIVIDUAL, INNOVATIVE & SECURE IT SOLUTIONS

MANAGEMENT LIFE CYCLE PROCESS

9 steps of a successful management

RITTER TECHNOLOGIE

1. PROVISIONING
2. RTU-INSTALLATION
3. NETWORK-CONNECTION
4. REGISTRATION
5. FINALISING META-DATA
6. SYSTEM-CONNECT
7. CONFIRMING
8. CHANGES
9. DEACTIVATION

Concept DeMaS

RTU MANAGEMENT TASKS

An overview of the most important remote terminal unit tasks

RITTER TECHNOLOGIE

COMMISSIONING

- DECOMMISSIONING

ADMINISTRATION

- CHANGE MANAGEMENT
- LOCATION MANAGEMENT

SYSTEM CONTROL

- CONFIGURATION (I.E. MAPPING)
- RTU MANAGEMENT (HW/SW)

MONITORING

PROVISION OF DATA FOR 3RD-PARTY SYSTEMS (I.E. SCADA)

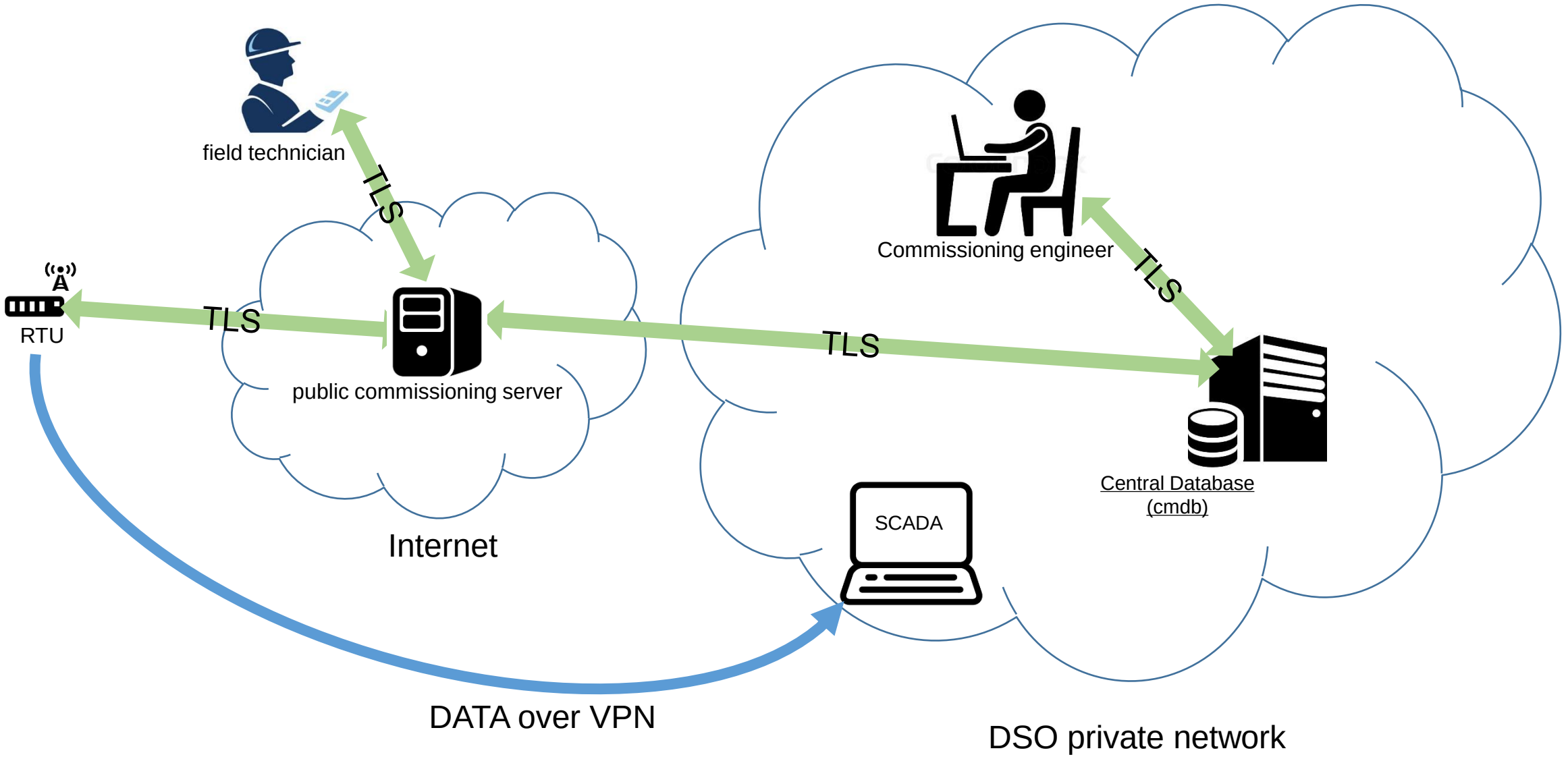
- INSTALLATIONS ORDER MANAGEMENT

Concept DeMaS

DEMAS PROCESS OVERVIEW

DEVICE MANAGEMENT SYSTEM

RITTER TECHNOLOGIE



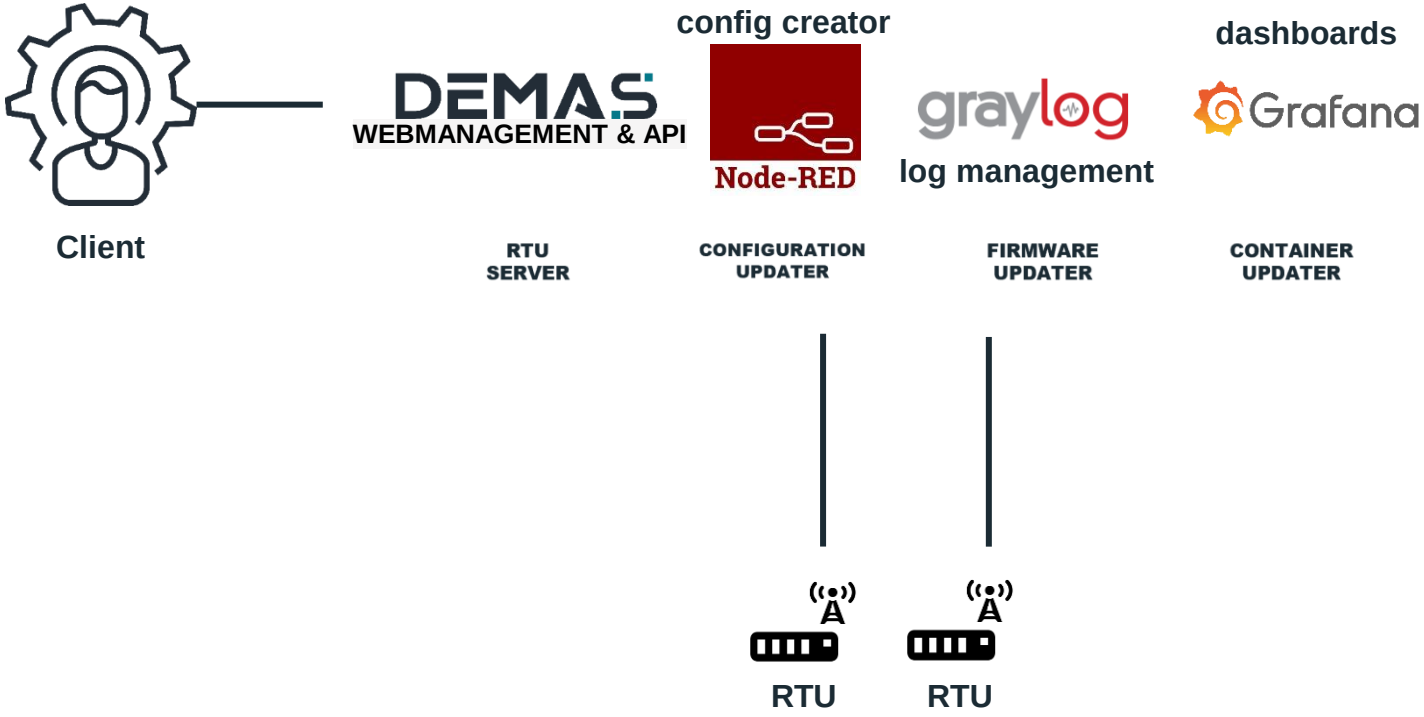
DEMAS OVERVIEW

DEVICE MANAGEMENT SYSTEM

RITTER TECHNOLOGIE

DEMAS

DEVICE MANAGEMENT SYSTEM

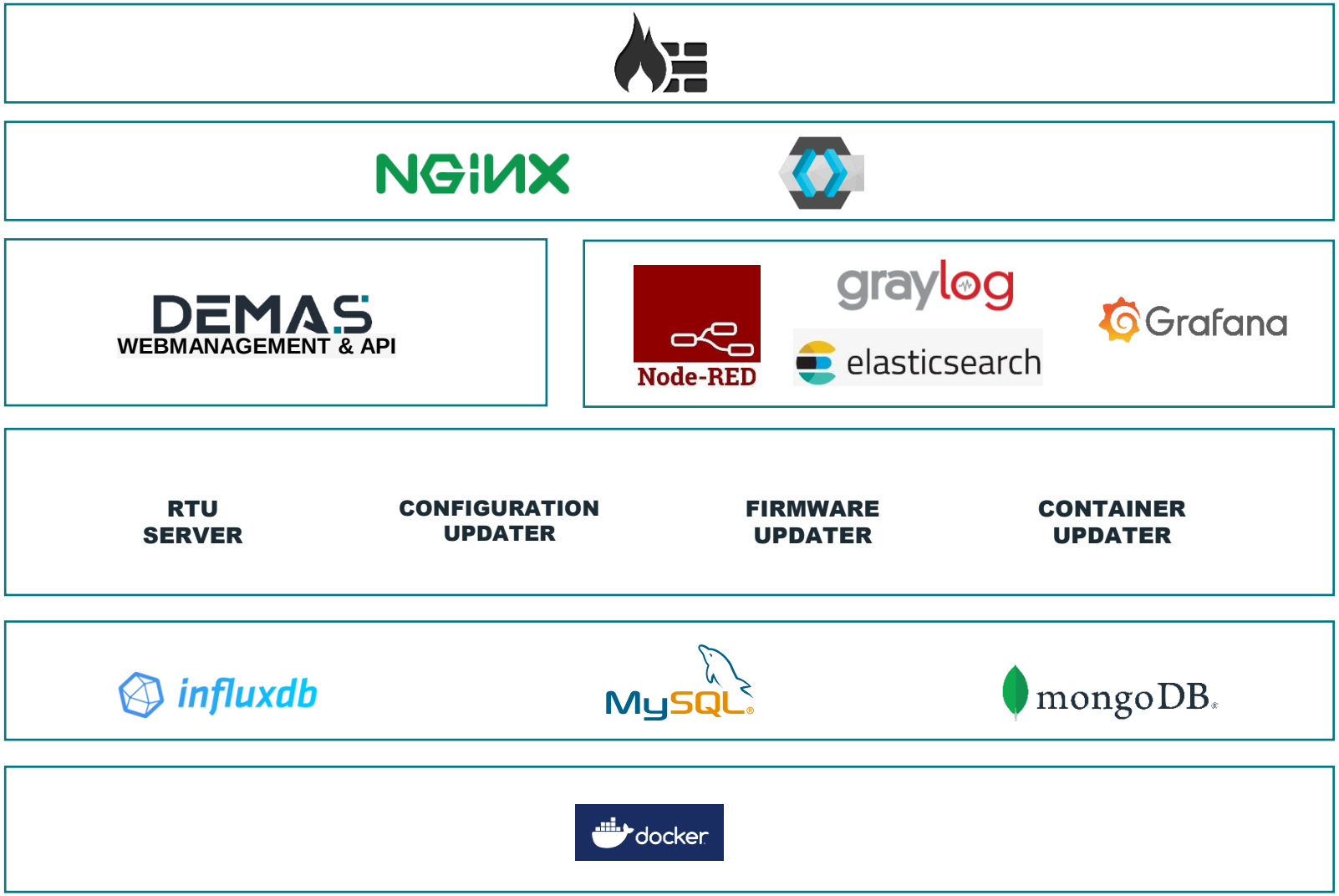


Concept DeMaS

DEMAS ARCHITECTURE

DEVICE MANAGEMENT SYSTEM

RITTER TECHNOLOGIE



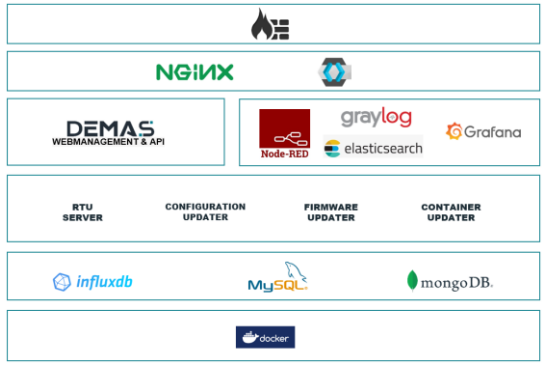
Concept DeMaS

HIGH AVAILABILITY

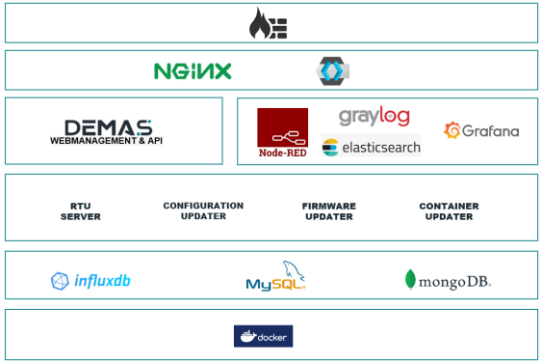
RITTER TECHNOLOGIE

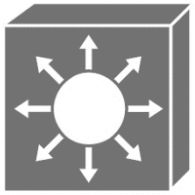
DEMAS DEVICE MANAGEMENT SYSTEM Datacenter 2

kubernetes

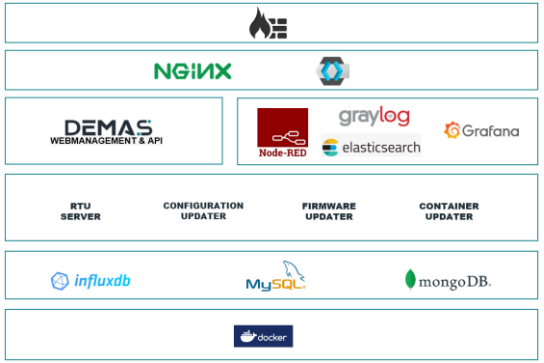


DEMAS DEVICE MANAGEMENT SYSTEM Datacenter 1





DEMAS DEVICE MANAGEMENT SYSTEM Datacenter 3

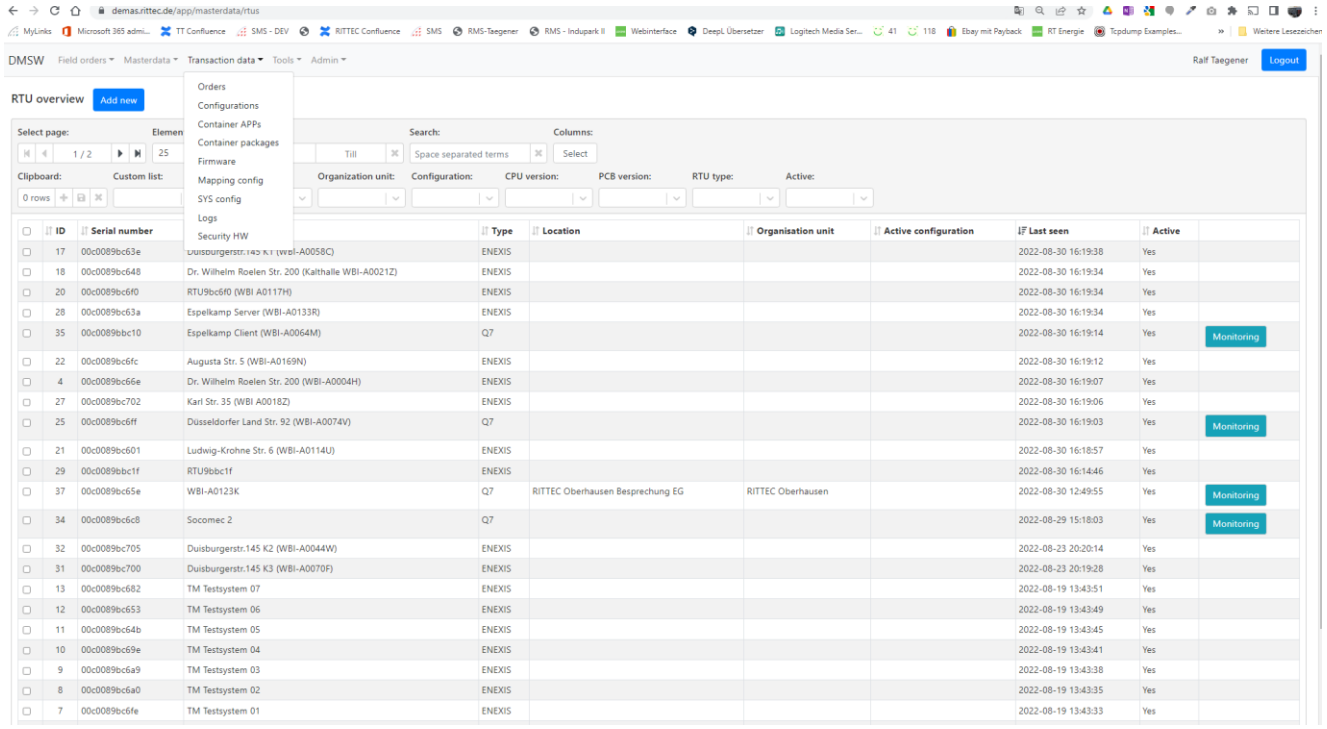


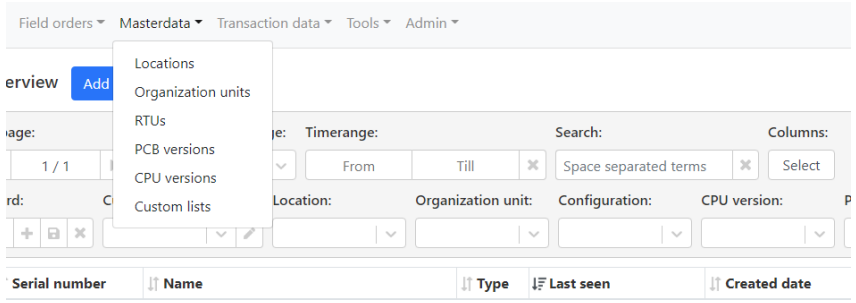
Concept DeMaS

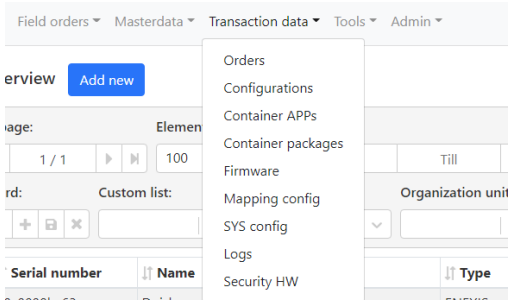
DEMAS WEBINTERFACE
DEVICE MANAGEMENT SYSTEM

RITTER TECHNOLOGIE

Master data & orders



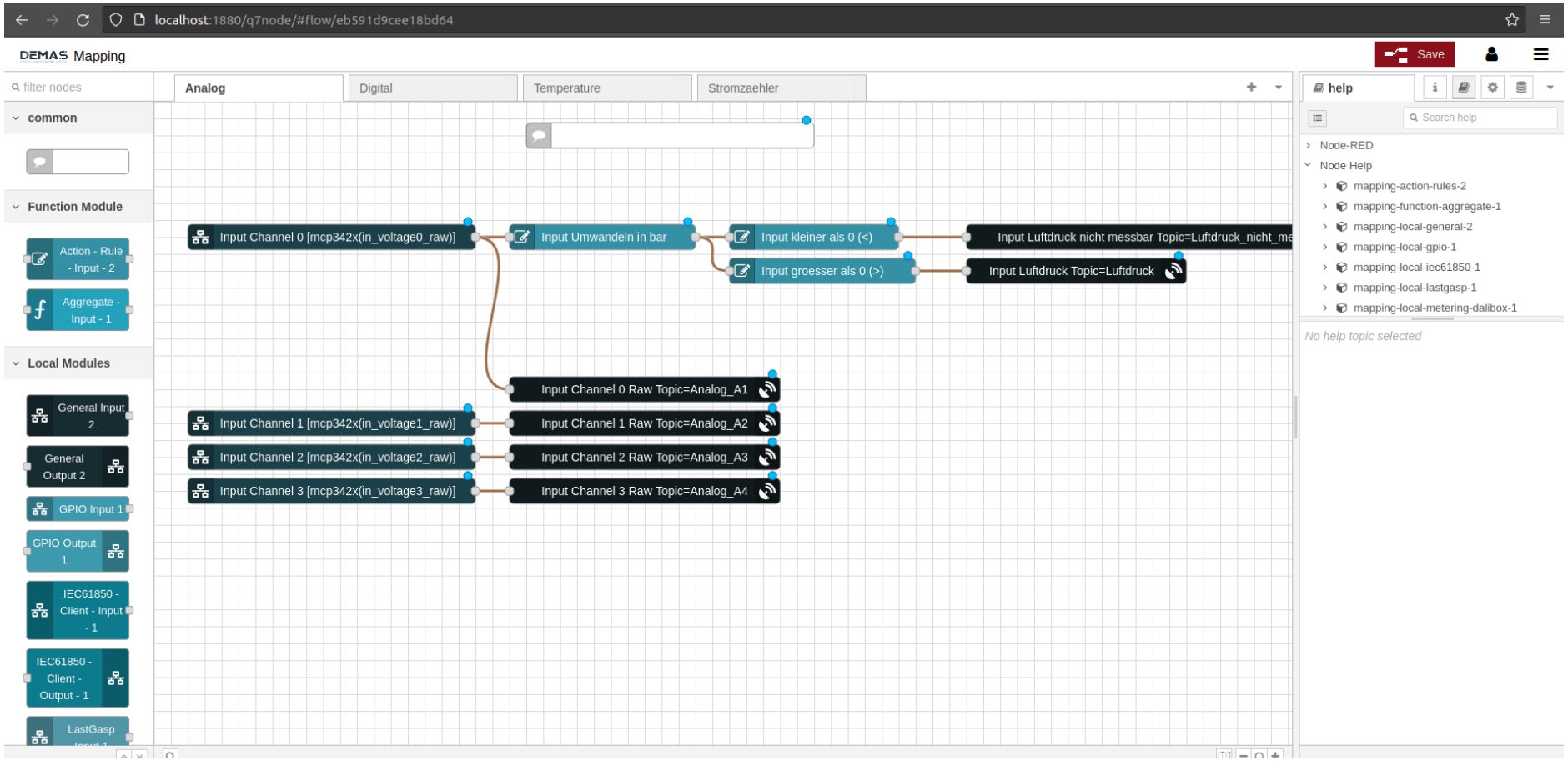




Concept DeMaS

MAPPING CONCEPT NODE-RED

Mapping over Node-Red export



Concept DeMaS

RTU STACK

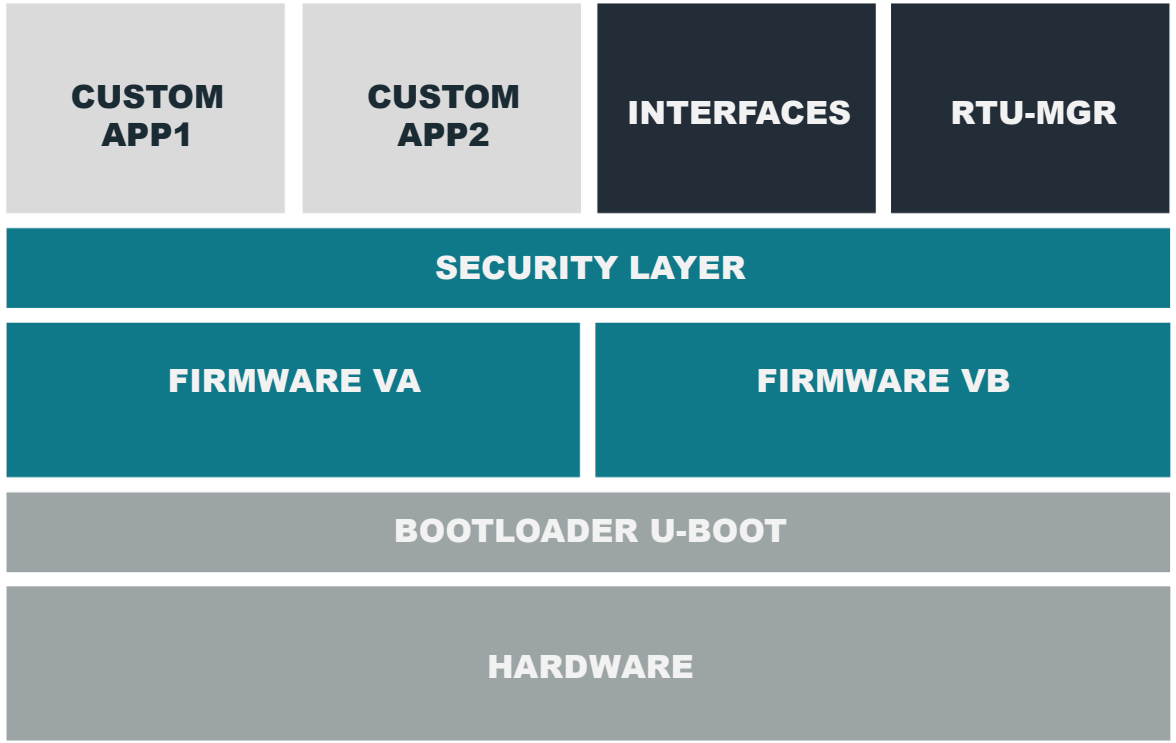
Schematic representation of the RTU system structure

CUSTOMER SOFTWARE TEAM

RITTEC SOFTWARE TEAM

RITTEC SECURITY TEAM

BAUSCH HARDWARE TEAM



Concept DeMaS

API SECURITY

RITTER TECHNOLOGIE

- The API provided by RITTEC includes a table that contains a "whitelist" function.
- External calls are translated to internal functions and processes after coordination.
- Individual functions can be activated / deactivated in the process.

Vendor Security

Vendor Security Maturity

ORGANIZATIONS AND ROLES

RITTER TECHNOLOGIE

RITTER passion4energy

ISO 27001 Certified Information Security Management System www.tuv-sud.com/ms-cert

EKu.SEC

CISO / ISB
Volker Brinkhoff

BAUSCH datacom

MANAGEMENTSYSTEEM CERTIFICATIE DNV·GL ISO 9001

QUALITY MANAGER
Dominiek Truyers

RITTER TECHNOLOGIE

ISO 27001 Certified Information Security Management System www.tuv-sud.com/ms-cert

CONCEPTEC®

CISO / ISB
Ralf Taegener

CENTRAL SECURITY
Ralf Kochems

CVE TEAM
David Siemko (Head)
Matthias Fehl
Thomas Muthmann

Vendor Security Maturity

OPERATION DESCRIPTION

RITTER TECHNOLOGIE

VB 23.3: MANAGEMENT OF SECURITY RISKS (CVE MANAGEMENT)

- 22.02-1 LTS dated 12/14/2021
- 2021-11-10 - CVE-2021-42321 - Vulnerability in Microsoft Exchange Server related to remote code execution - (IMS-490)
- CVE Team RTU (Matthias Fehl and Thomas Muthmann)

Vendor Security Maturity

In our CMDB (part of the Service Management System) the used libraries are recorded. We learn about vulnerabilities through the approved bodies and vendors. The closure of vulnerabilities is essentially dependent on support from the manufacturers or communities.

Among other things, the security team evaluates the recommendations of the Mitre / Nist and informs the customers about the possible risks and solutions. As long as no definitive solutions exist, possible alternatives or workarounds are coordinated with the customers.

Response time for this information: max. 3 working days

Yes, there is a charge for this service, as the effort required to find solutions has increased significantly in recent years.

SECURITY MEASUREMENT

The entire RITTEC organization is certified according to ISO 27001:2017. Thus, both the Infrastructure, Software Development and Support departments work according to fully certified workflows.

Vendor Security Maturity

FROM THE MITRE / NIST RECOMMENDATIONS

- Stability of the component in terms of functionality
- Mainly use open source products to perform own source code reviews (if necessary create a fork)
- Use only active projects.

The biggest risk is in case of abandonment of the open source projects. In this case further developments must take place in the own house, or it must be changed to alternative products.

EXTERNAL SECURITY TESTING

RITTER TECHNOLOGIE

The products are tested and proved by:

TROVENT SECURITY GMBH
Zentrum für IT-Sicherheit
Lise-Meitner-Allee 4
44801 Bochum, Germany

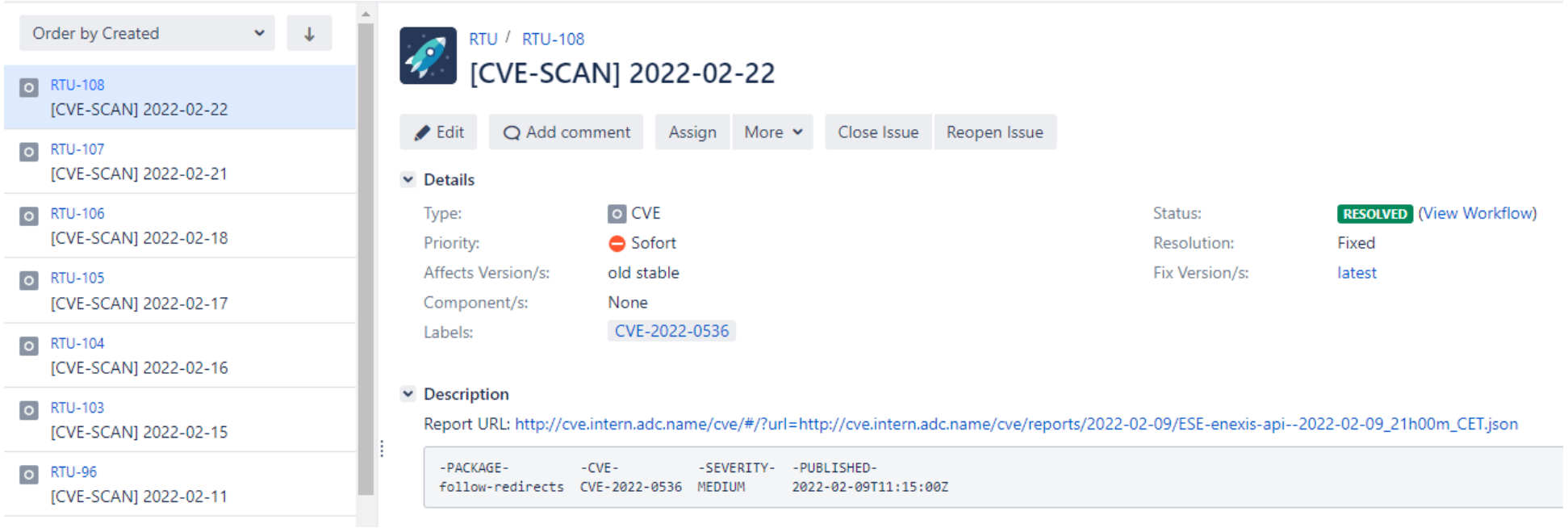
Vendor Security Maturity

VULNERABILITY SCANS

RITTER TECHNOLOGIE

We have already implemented a procedure to check all code repositories for new CVEs on a daily basis. For this procedure, Trivy is used, which automatically publishes reports and creates them in tickets for the appropriate departments. The Trivy integration for Buildroot will be done through a parser for the PKG stats created by Buildroot.

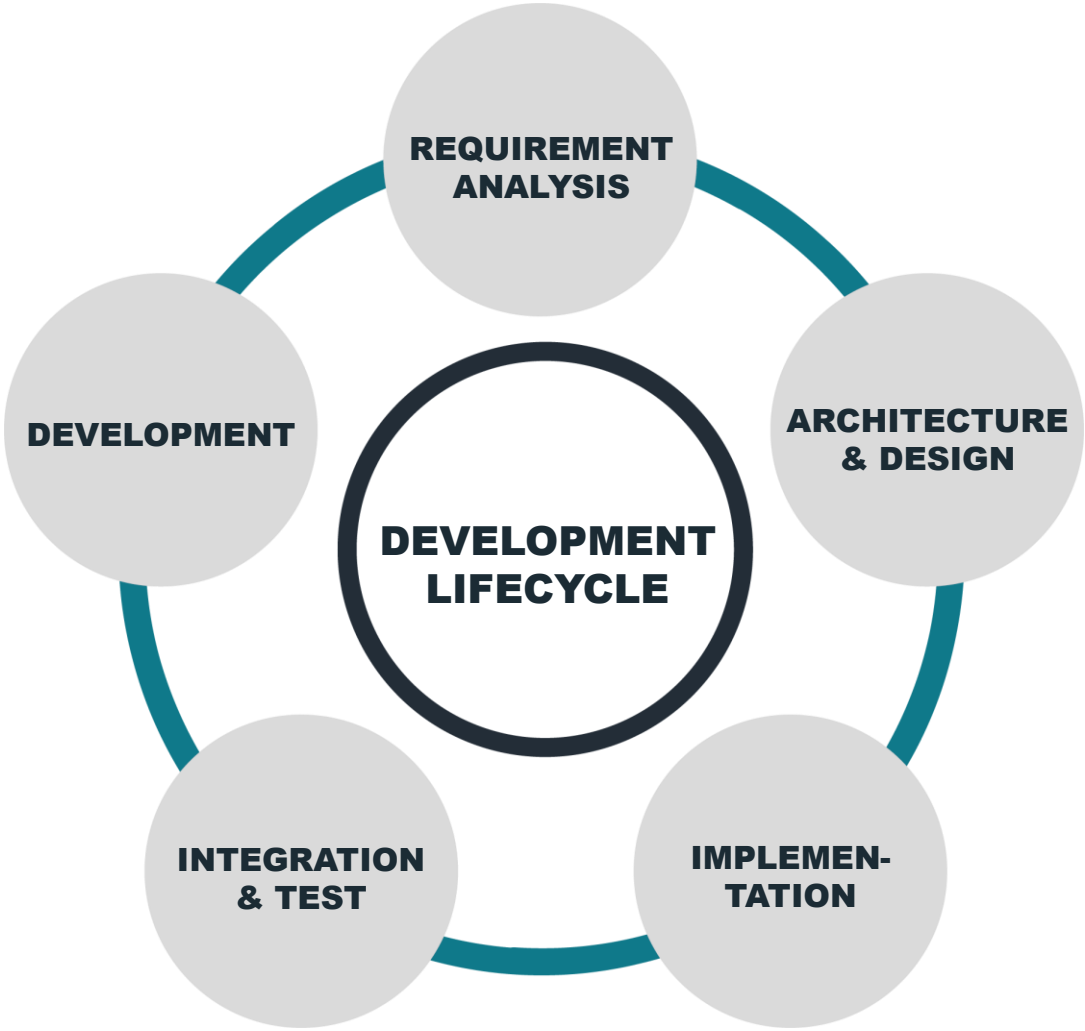
Vendor Security Maturity



SECURITY FIRST DESIGN LIFECYCLE (SDLC)

RITTER TECHNOLOGIE

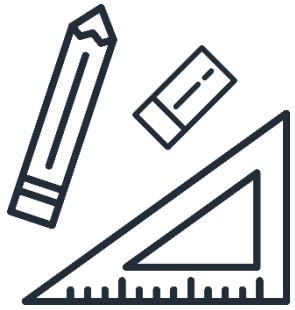
- Secure concepts: e.g. CRS, OWASP against SQLi, XSS, LFI, RFI, PHPci
- Using BSI standards 2020
- Manual and automatic tests e.g. Cypress / Postman
- 27K certified data center and hardware / software development

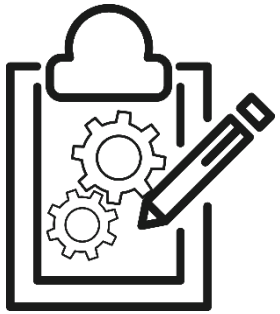


Vendor Security Maturity

SIMPLE PROCESS, STRONG RESULT

RITTER TECHNOLOGIE





Vendor Security Maturity

DRAFT PHASE → **REFINEMENT AND DOCUMENTATION** → **REALISATION**

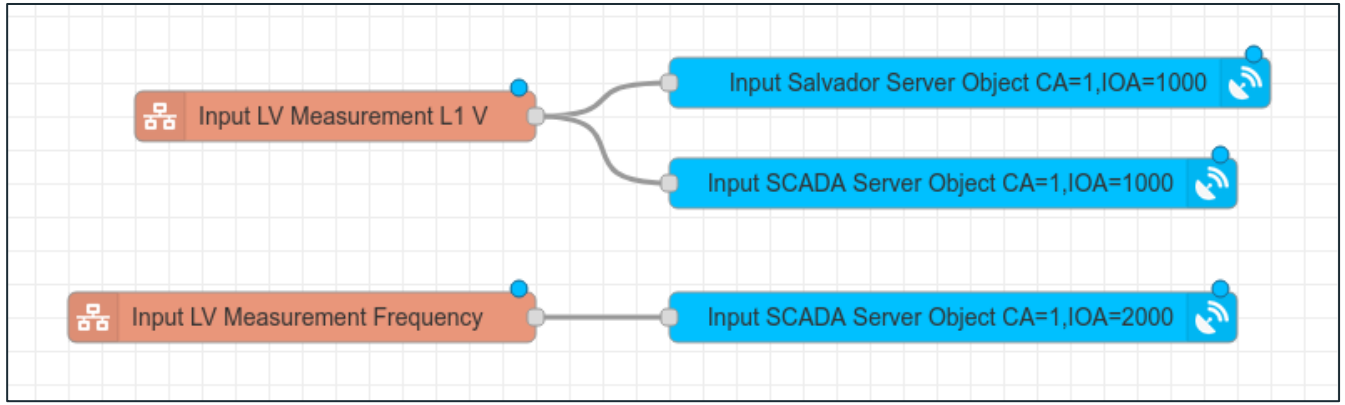
- Full integrated Atlassian Jira and Confluence based processes for system and software development controlled by an integrated Quality System (iQS)

- CVE
- Scrum
- Documentation standards

ACCESS RIGHTS IEC 60870-104

RITTER TECHNOLOGIE

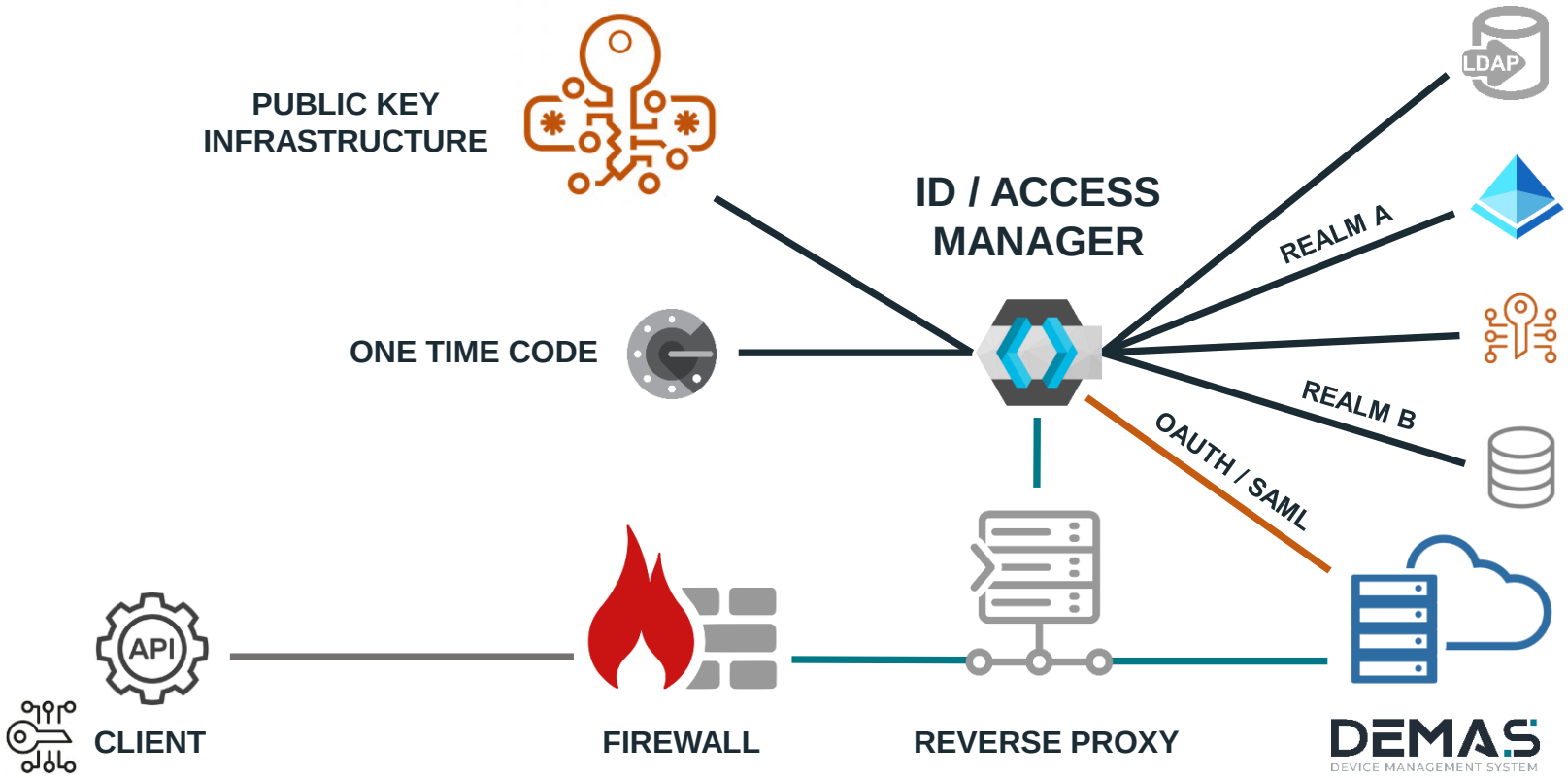
Each IEC60870-104 server process is able to connect to only 1 client, redundant passive connection excluded. If several client systems like Salvador and SCADA want to connect to the RTU, it is therefore necessary to have 2 IEC6087-104 server processes running on the RTU. This can be done via the mapping file by creating 2 configuration objects. Each IEC60870 server process has its own IOA object space. If you want to provide monitoring / control objects for both 104 server processes, it is necessary to create 2 objects within the mapping. 1 object for each server.



This procedure makes it possible to specify exactly which monitor and control objects are to be provided for each server process. An IP filter is provided for this purpose.

ACCESS CONTROL

RITTER TECHNOLOGIE



Product Security RTU

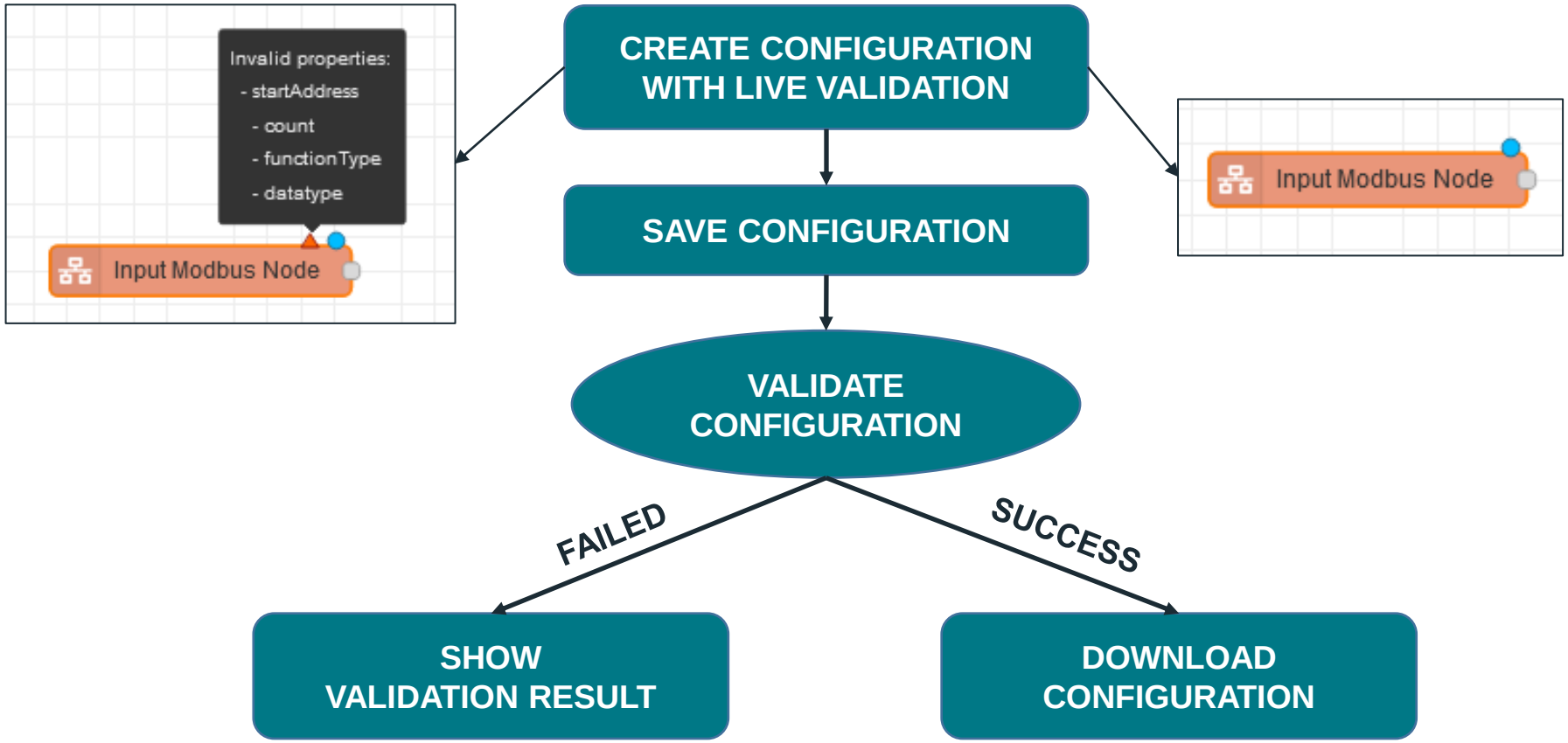
ACCESS CONTROL (SCADA)

RITTER TECHNOLOGIE

Access based on IP filter, secured by Ipsec VPN

VALIDATION OF CONFIGURATION FILES

All configurations are provided from Node-Red and will be automatically checked.



KEY AND CERTIFICATE MANAGEMENT

RITTER TECHNOLOGIE

During initial startup and when the expiration date is reached, the RTU retrieves a certificate from the PKI server via SCEP. This certificate is used to establish the IPsec connection from the RTU to the Customer network. It is also optionally used for communication between the RTU and DEMAS.

Requirement: Provide a matching Root CA
for DEMAS, since Customer PKI generates the certificates.

OPTIONAL DUE TO REQUIREMENTS

- Security - Confidentiality
  and integrity of network communication: on RTU

- If the WAN connection is already secured via VPN,
  optionally disable further encryption and thus
  of course certificates for deep packet inspection.

ACCESS CONTROL FOR ENGINEERS (DEMAS)

RITTER TECHNOLOGIE

The structure of our technical protection is generic. All auth providers can be connected via Keycloak and NGINX.

We have chosen mTLS (TLS client certificate issued via local PKI (SCEP)).

In addition to DEMAS, other arbitrary systems can optionally be secured with this generic concept.

ACCESS CONTROL FOR ENGINEERS (RTU)

RITTER TECHNOLOGIE

The RTU is centrally managed by DEMAS. Therefore, direct access to the RTU via SSH is possible, but not required. With the RTU it is possible to define arbitrary users, passwords and group assignments in the system configuration.

A central login service manages the logins for the DEMAS and Node-Red modules. This configuration is normally provided by DEMAS, but can be changed locally. In that case, the change is detected and UUID 0 is reported back to DEMAS. This allows DEMAS to react to the change.

The files and fatal recovery scripts can only be changed or executed by users with root rights.

So the user must be either in the root group or the sudo group. In the second case, the user must initiate all actions with sudo.

WAN SECURITY

RITTER TECHNOLOGIE

We use Strongswan IPsec to secure the WAN communication path from the RTU to the Customer network. The configuration of the IPsec parameters can be defined in the system config.

The certificate used is fetched from the PKI server during initial access and expiration via SCEP.

Authentication between 104 server and client is not implemented yet, because it is not part of the protocol specification

To secure the communication, we are using IPsec for confidentiality and integrity.

RTU SECURITY FEATURES

RITTER TECHNOLOGIE

- FIT (Flattened Image Tree)
  - Hashed: SHA-256
  - Encrypted : AES-256-CBC
  - Signed X.509 Cert (4096 Bit RSA Key)
- Cert check and image decryption on boot
- Bootloader is secured via HABv4 signature (closed source by NXP)
- CPU provides a HABv4 secure boot feature
- CPU loads only bootloader with correct HABv4 signature
- Dual boot for firmware fall back
- Cert programmed in OTP (One Time Programmable) fuses

FIRMWARE SECURITY - PART 1

RITTER TECHNOLOGIE

The RTU firmware uses the FIT format. This one file contains the kernel, the device tree and the root filesystem. The RTU uses a RAM filesystem to prevent corruption of the root FS. The bootloader U-Boot checks the validity of the firmware FIT image at every boot, unpacks the data into RAM and executes the Linux kernel. All changes in the root FS are lost after a reboot.
The rtu-mgr process sets the settings for all services at each boot according to the system config provided by DEMAS.

The FIT image is signed accordingly. The public key is in the boot loader because it must verify the image. The private key is only on the RITTEC firmware build server and does not leave it.

We use the maximum key format supported by U-Boot RSA 4096 bits with SHA256.
The data in the FIT image is encrypted and the corresponding key is only obfuscated in U-Boot. This is not security relevant, only a measure against reverse engineering.

FIRMWARE SECURITY – PART 2

RITTER TECHNOLOGIE

Furthermore every FIT image gets a HABv4 signature. This is a proprietary procedure from NXP, implemented in the CPU. For this a private and public key is generated with a NXP tool. The private key never leaves the build server. The public key is burned into the CPU by OneTimeProgrammable Fuses.

After the CPU is permanently closed via another OTP fuse, it can only execute correctly HABv4 signed bootloaders. The bootloader U-Boot we use is therefore HABv4 signed just like the firmware FIT image. After loading the FIT image, the bootloader first checks the HABv4 signature with the help of the CPU, then the FIT signature, decrypts the data into RAM and starts the kernel.

A firmware update is performed by overwriting the complete inactive FIT image. The previously inactive image is activated and rebooted.

All the operations described above now follow. If the image does not start for whatever reason, the watchdog switches back to the old image.

HARDENING RTU

RITTER TECHNOLOGIE

1. RUNNING PROCESSES AT STARTUP

- auditd (Audit Daemon)
- dbus (DBUS Daemon)
- nftables (Firewall)
- rtu-mgr (Connect to DEMAS and Setup System)
- Systemd
- watchdog

Product Security RTU

2. RTU-MGR NOW CONFIGURES AND STARTS OTHER SERVICES ACCORDING TO THE SYSTEM CONFIG

- docker (container daemon)
- lighttpd (webinterface for initial setup)
- ModemManager and pppd (LTE modem)
- mosquitto (MQTT daemon, internal only)
- NetworkManager
- ntpd (NTP Daemon)
- serial-getty (Debug Console)
- sshd (SSH Daemon)
- strongswan-starter (IPsec Daemon)
- telegraf (Send Data to Grafana)
- wg-quick (Wireguard Daemon)

HARDENING RTU

RITTER TECHNOLOGIE

3. RTU-MGR ALSO CREATES THE LINUX USERS AND PASSWORDS ACCORDING TO THE SYSTEM CONFIG, SO NO ACCESS IS POSSIBLE BEFORE

We use a local fork of Buildroot for the firmware build, so we can use our own updates in addition to the normal Buildroot updates to react quickly to important CVEs.

As kernel we use Linux Mainline LTS 5.10 with PREEMPT_RT realtime patches.

The complete firmware is compiled with ASLR/PIE, RELRO, SSP, Seccomp, FORTIFY SOURCE Protection.

RITTER
TECHNOLOGIE

CONTACT

RITTER TECHNOLOGIE GMBH

Essener Straße 2-24
46047 Oberhausen, Germany
Phone: +49 208 85 96 230

SEBASTIAN HAHN
sebastian.hahn@rittec.de

RALF TAEGENER
ralf.taegener@rittec.de

THOMAS MUTHMANN
thomas.muthmann@rittec.de

DAVID SIEMKO
david.siemko@rittec.de