STAKEHOLDER-ORIENTED ELABORATION OF A SECURE AND SAFE SOFTWARE UPDATE PROCESS USING SYSTEMS ENGINEERING METHODS

SWISSED25 - Stories Experienced

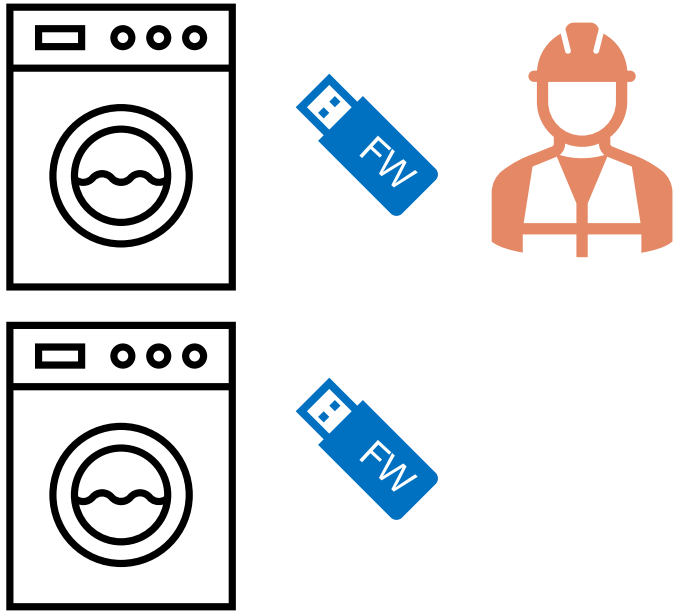
Ivo Locher, Andy Tonazzi
Sept 15, 2025

ilkonplan

GOAL OF THE PROJECT

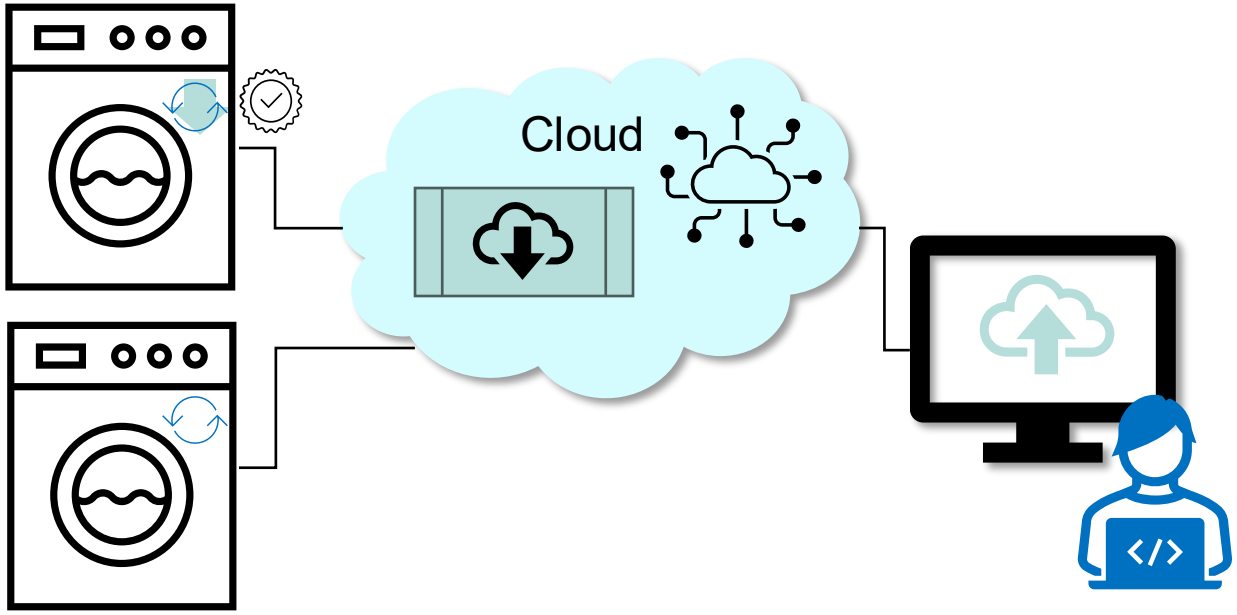
Current situation

Service technician updates firmware of machines on-site



Intended situation

Secure remote update functionality for machines.
Update approval at machine.



WHY IS A REMOTE UPDATE FUNCTION NEEDED?

- Faster roll-out of security patches
- Improves efficiency
- Allows focusing on more “value creating tasks”

Law:

- EU Medical device regulation → IEC 81001-5-1, etc.
- FDA → various guidance documents
- EU Cyber resilience act (end of 2027) → IEC 62443, etc.

→ no market clearance of products containing software without update feature

APPROACH

- Elaborate high-level stakeholder map to identify constraints (customer, hospital, ..)

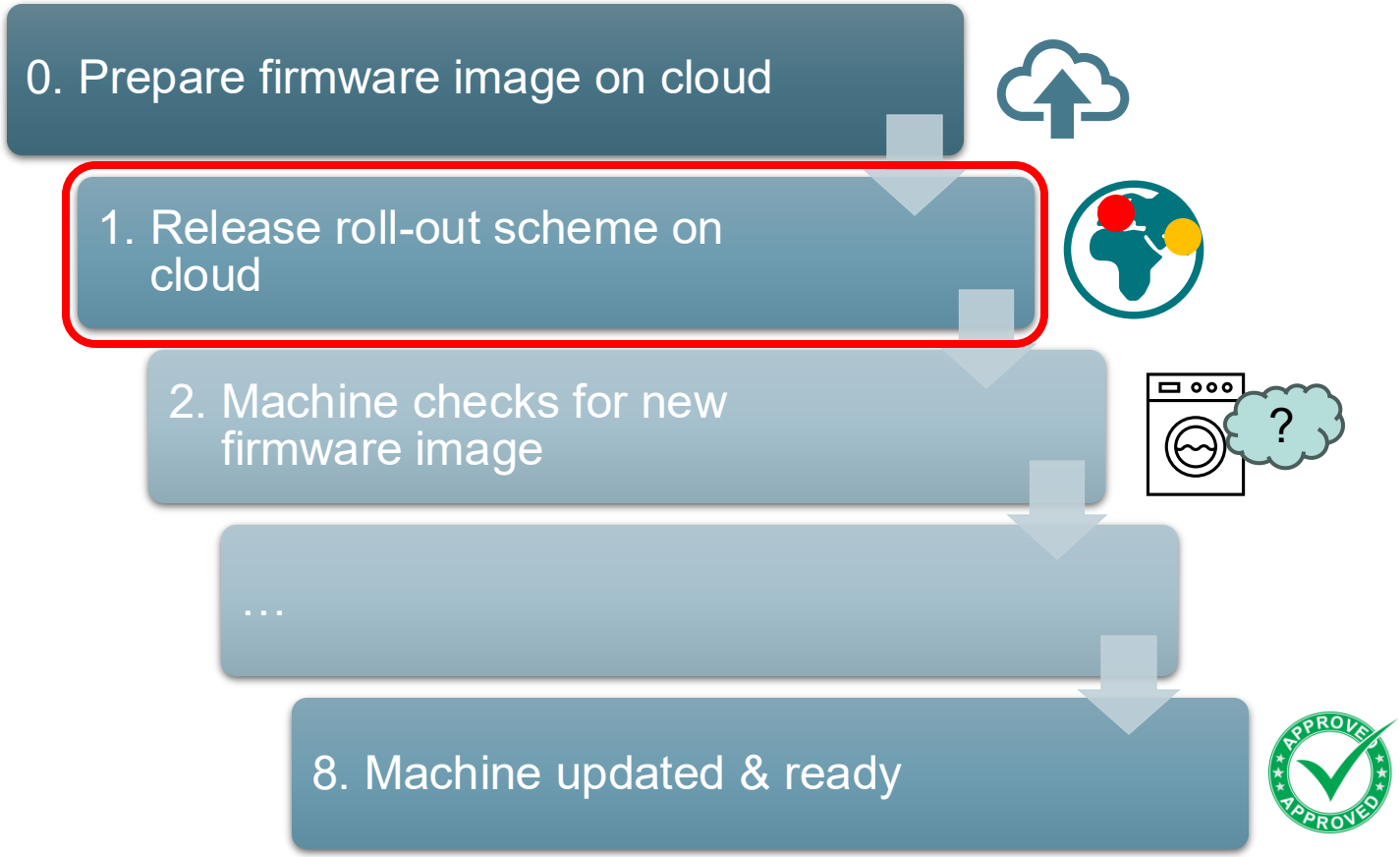
- Assess security along the product lifecycle stages

- Define secure remote Firmware update process
  - Ensure a secure and safe update workflow
  - Identify new roles and new stakeholders
  - Elaborate secure system architecture
  - Include security schemes and technologies

SECURE AND SAFE FIRMWARE UPDATE WORKFLOW

Iterative elaboration of the remote firmware update workflow by considering:

- Identified stakeholders
- Organizational constraints
- Deep dives for each step of the workflow
- Best-practice safety
- Best-practice security



DEEP DIVE FOR EACH STEP IN THE UPDATE WORKFLOW

Elaboration of the task lists and end-to-end use cases (workflows), e.g.

3.2. Details to Step 1: Activation of Firmware image update roll-out

Sub-step	Details
1. Authentication and Authorization: The "Product Owner Firmware" logs into cloud.	The login shall require Two-Factor Authentication. Connection is secured/encrypted.
2. "Product Owner Firmware" uploads the firmware image to cloud. Progress is depicted.	The release is stored on cloud in a secure storage.
3. Once upload has finished, Cloud service checks the firmware image signature and integrity. Pass/Fail is depicted to the "Product Owner Firmware".	• This step ensures that the firmware image has been uploaded uncorrupted. The public key for the signed firmware image is used for this step. • Furthermore, it is verified that the firmware image version is appropriate (e.g. version number higher than latest stored version, all required files

Use case

Implementation details

NEW ROLES AND NEW STAKEHOLDER IDENTIFIED

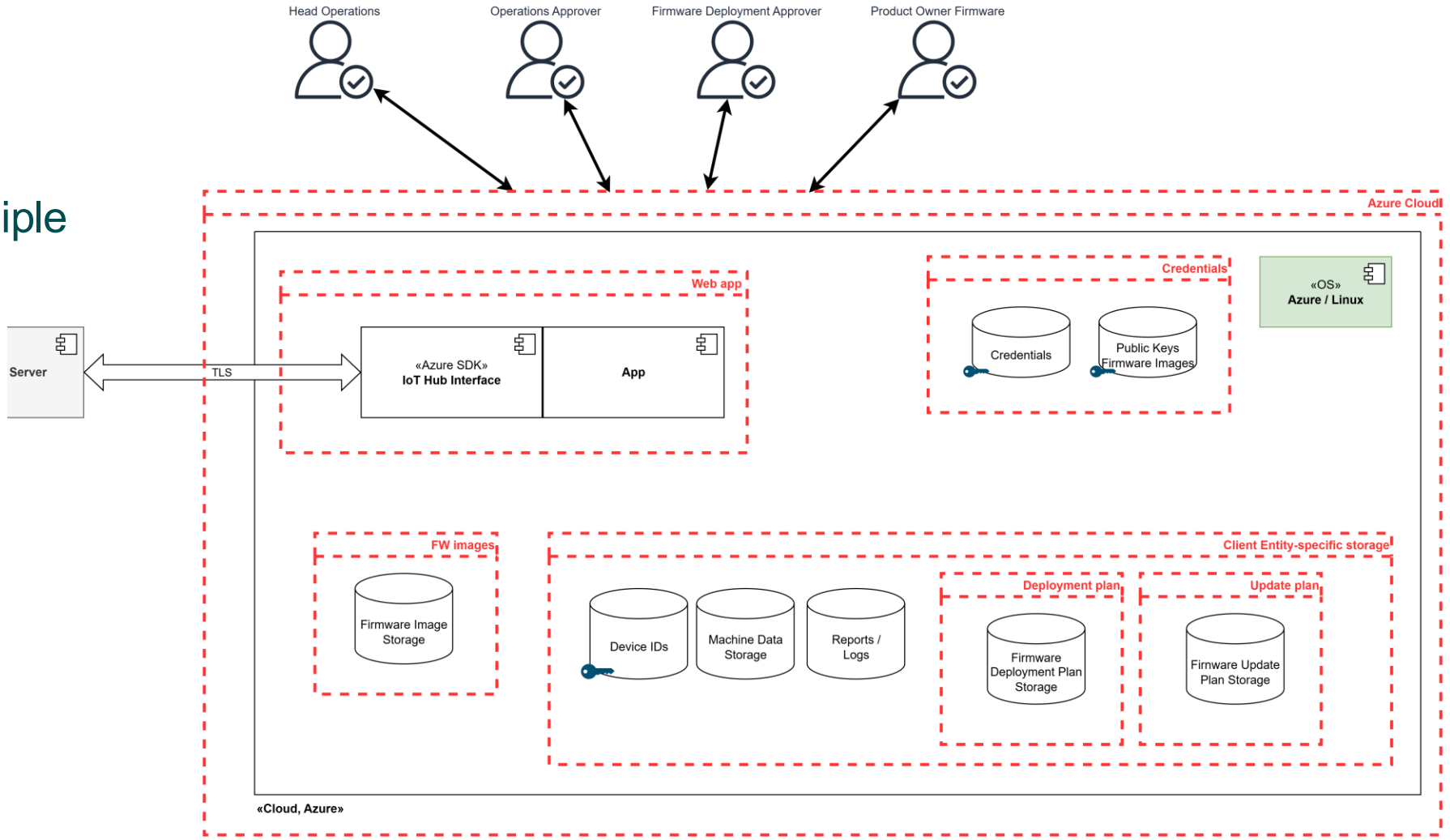
Elaboration based on the workflows, e.g.

- Who is eligible to upload a new firmware release to the cloud?
- Who defines the roll-out scheme, who approves the scheme?
- Who needs to be informed about the success of the update?
- …

Role	Entity	System	Privileges
PO Firmware	[redacted]		Uploads the firmware images and configurates the update process. Configures the roll-out scheme.
Service Team	[redacted]		Configures the roll-out scheme for its local entity base
Firmware Update Approver	[redacted]		Approves the firmware update configuration and roll-out scheme

INTEGRATION FOR SECURE SYSTEM ARCHITECTURE

- Defense-in-depth concept (for assets)
- Least privileges principle



SECURE ARCHITECTURE – THREAT MODELING

- Modeling of technical update process using Data Flow Diagrams (DFD)
- Threat Modeling using pseudo-standard STRIDE

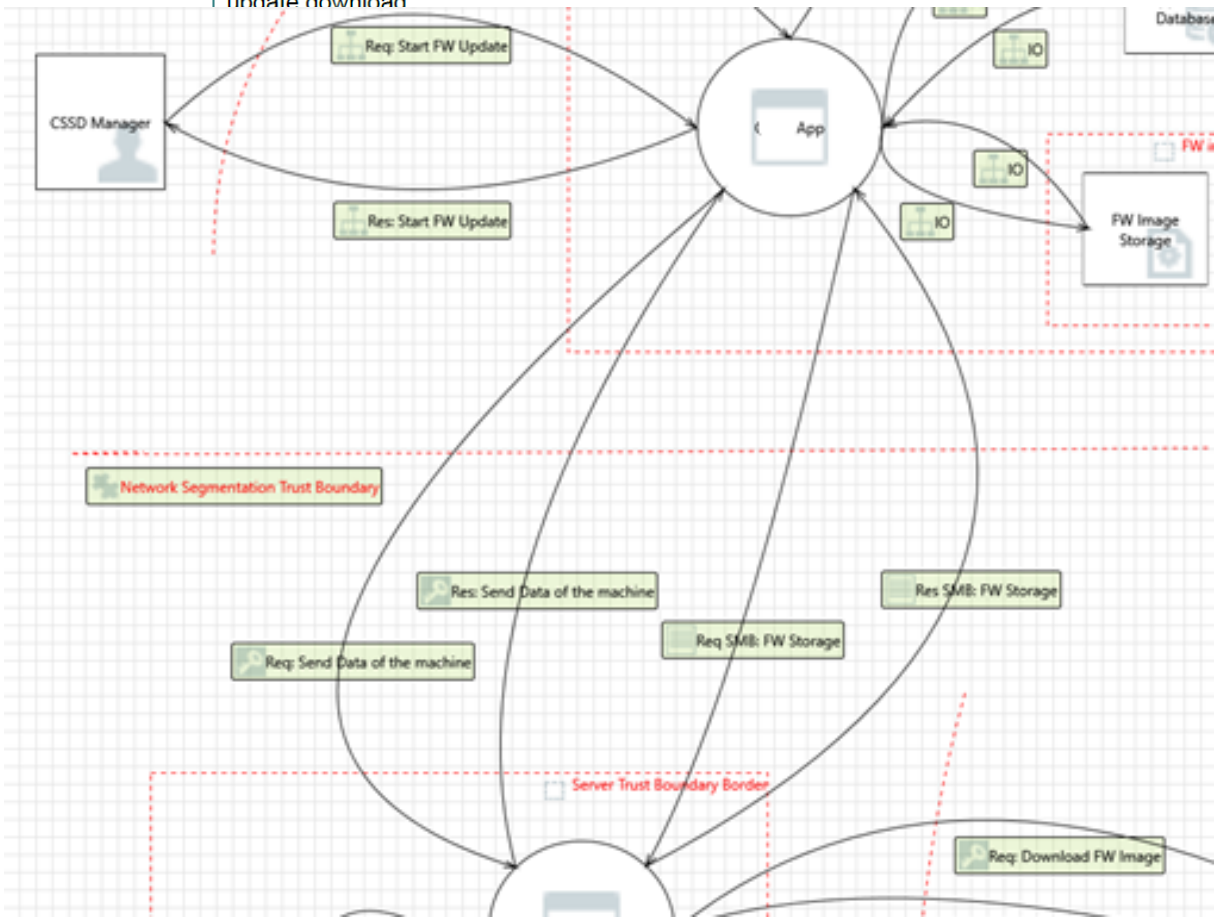
Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

- Identification of potential vulnerabilities in the design
- Proposing risk control measures

➔ Very long list of repetitive security control measures

➔ Starting at “zero”

Asset	Confidentiality	Integrity	Availabili
App / IoT Hub	Medium	High	Medium
FW Image Storage	Medium	Medium	Medium
Credentials Login SHO	High	Medium	Medium
Public Keys FW Images	Low	Medium	Medium
Credentials SHO, for FW update download	High	Medium	Medium



IDEA FOR DISCUSSION: ASSURANCE CASE APPROACH

Assurance Cases: AAMI TIR 38, ISO/IEC 15026

Structure:

- Claim
  - Arguments (why)
    - Evidences

→ Starting from the “End”

→ **“Security Assurance Case”**

Example:

Claim 1: The web portal is sufficiently secured

- Argument 1: The security of the portal is maintained.
  - Argument 1.1: Com. is encrypted using TLS
    - Evidence: review → https connection
  - Argument 1.2: Authentication using 2FA
    - Evidence: Test case xy
  - Argument 1.3: Access rights managed by user roles (privileges)
    - Evidence: Penetration test
  - Argument 1.4: …

- Stakeholder-friendly presentation of the remote firmware update workflow:
  - Product Owner
  - Service engineer
  - System architect
  - Software engineer

- Enables discussion about the workflow across all levels
  - User level
  - Organizational and process level
  - Security and safety level
  - Implementation level

- Tangible results by providing a secure architecture and “recipes” for implementation

THANK YOU

Please visit us at the booth outside !

Andy Tonazzi
Owner / CEO

linkedin.com/in/andy-tonazzi-konplan

+41 41 799 30 10

andy.tonazzi@konplan.com

konplan

Ivo Locher, PhD, EMBA, PMP
Program Manager at konplan

https://www.linkedin.com/in/ilocher/

+41 41 799 30 10

ivo.locher@konplan.com

konplan