Securware 2019, Nice, France

Panel on Security
Topic: Complexity of (Cyber-) Security

Moderator

Steffen Fries, Siemens AG, Germany

Panelists

Sebastian Fischer, Fraunhofer AISEC, Germany

George Yee, Aptusinnova Inc. and Carleton University, Canada

Reiner Kriesten, University of Applied Sciences - Karlsruhe, Germany

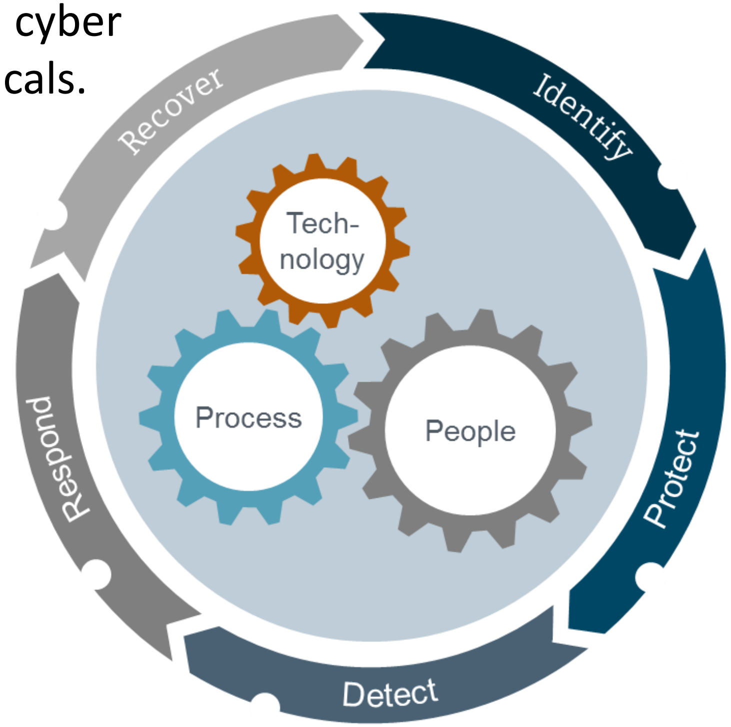
October 28th, 2019

complexity of cyber security

During development, integration, and specifically during operation of products and systems, different aspects of cyber security have to be considered (processes, technology).

Specifically as the interconnection between and integration of systems increases, cyber security becomes more and more a cross cutting topic through the different verticals.

- Examples for security considerations (no order, not complete)
  - development processes
  - functionality determination
  - supplier selection (supply chain security)
  - cryptographic algorithm agility
  - commissioning and deployment
  - user interaction with the system during operation and maintenance
  - patch management
  - …
- **One goal is therefore: Security by design and Security-by-default**



topics from the panelists

Sebastian Fischer, Fraunhofer AISEC, Germany

„How to find the appropriate level of security for each type of device based on guidelines and standards for cyber security"

George Yee, Aptusinnova Inc. and Carleton University, Canada

"Is complexity necessary for better security? Is complexity sufficient for better security?"

Reiner Kriesten, University of Applied Sciences - Karlsruhe, Germany

„Leveraging security experiences of the automotive industry in the IoT world based on the examples like SW-updates, integration of personalized services and apps, keyless go systems, and wireless tire pressure monitoring.„

Steffen Fries, Siemens AG, Germany

„Simplified but secured user-device interaction: Reducing complexity of secure device onboarding in IoT environments."

conclusion from the panel discussion

- Complexity seen with different impact
    - System internal: higher complexity may go along with a higher rate of exposures, which may be exploited by a potential attacker. This is bad for security.
    - System external: User interface for interacting with security should be designed in a way to make the interaction as easy as possible (best transparent) to be less error prone. In any case, security failures need to be provided in an understandable way. This may be different for the consumer and industry domain.
    - Security control: Complexity in the security control may be good for security (e.g. passwords) or bad for security (e.g. PKI) depending on the control. Having more complexity in a security control is never sufficient for perfect security (which doesn’t exist anyway).
    - Standardization of a security control for manufacturing products needs to be done carefully as it could allow attackers to use the same attack on multiple products if the attack is successful on one product.
- Security targets are different, depending on the use case. A threat and risk analysis is typically a sound base to derive security requirements for the intended use case. Note that the approach in cryptography is typically to publish the algorithm an rely on the secrecy of key information. But here also, the implementation matters.
- Ensuring security in products was discussed as very important. This may be supported by different activities for standardization of security functions and also by the definition of certification schemes allowing manufacturer based certification or certification by an independent auditor. It will be very difficult to have a truly independent third party to act as an international security auditor.
- Holistic security concepts were discussed as way forward to address greenfield and brownfield installation to an appropriate extend.

Fraunhofer
AISEC

“How to find the appropriate level of security for each type of device based on guidelines and standards for cyber security”

Sebastian Fischer (Fraunhofer AISEC, Germany)

28. Oct 2019

IoT Security Standards

- Germany: DIN SPEC 27072 (Consumer IoT)
- Europe: ETSI EN 303 645 (Consumer IoT)
- US: NISTIR 8259 (Consumer IoT)
- IEC 62443 (Industrial IoT)
- …

Challenges

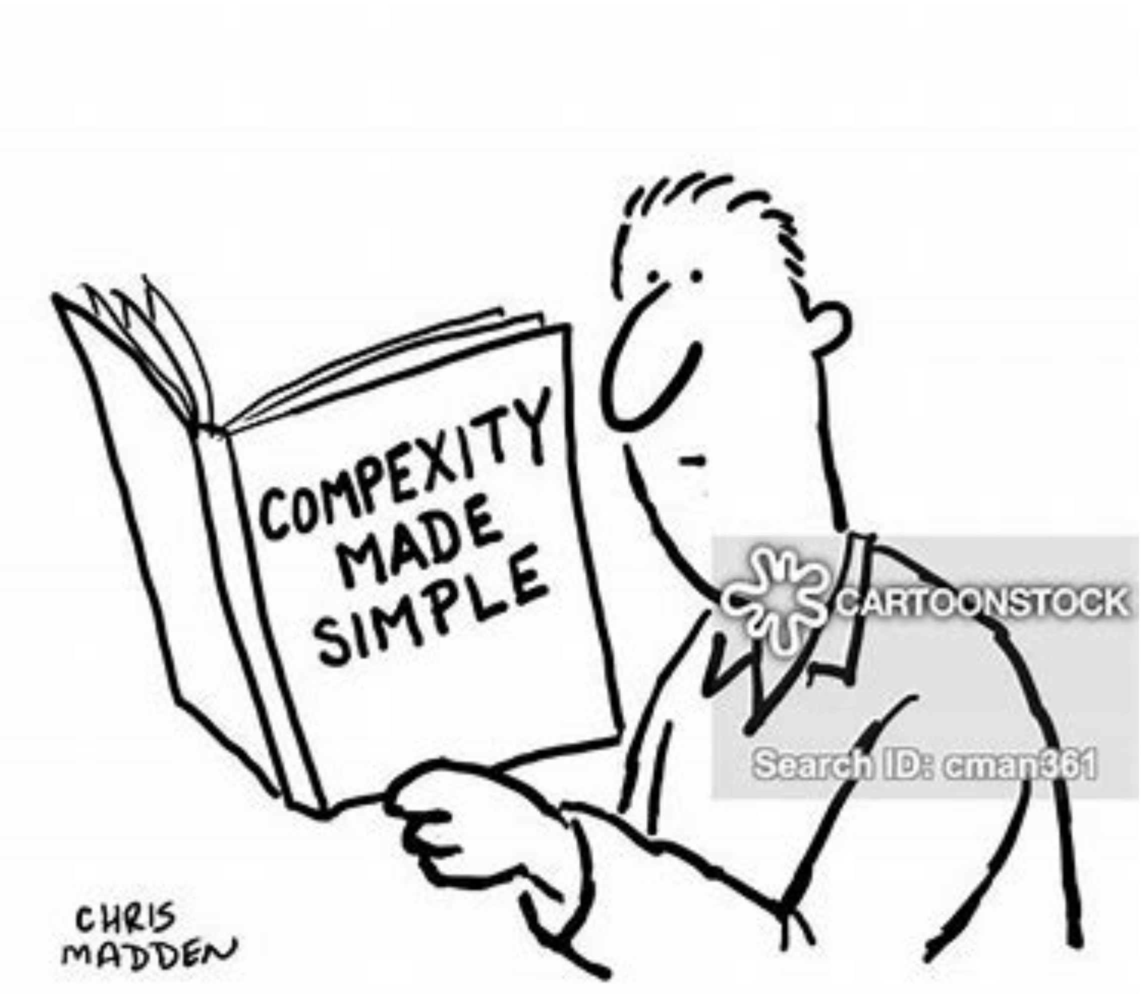
- Apply security to IoT devices
- Cheap devices need minimum requirements
- Are the standards for consumer IoT devices enough?
- **“How to find the appropriate level of security for each type of device based on guidelines and standards for cyber security”**

Security and Complexity

George Yee

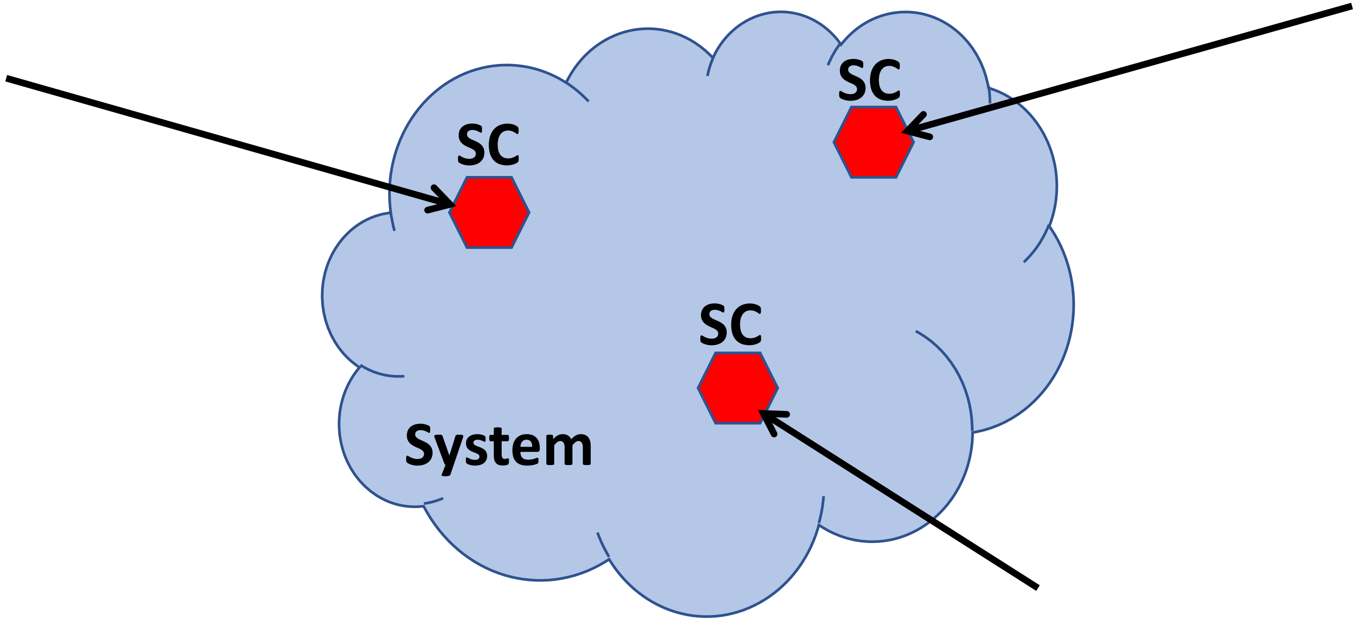
Aptusinnova Inc. and Carleton University

Ottawa, Canada


COMPEXITY
MADE
SIMPLE
CHRIS
MADDEN

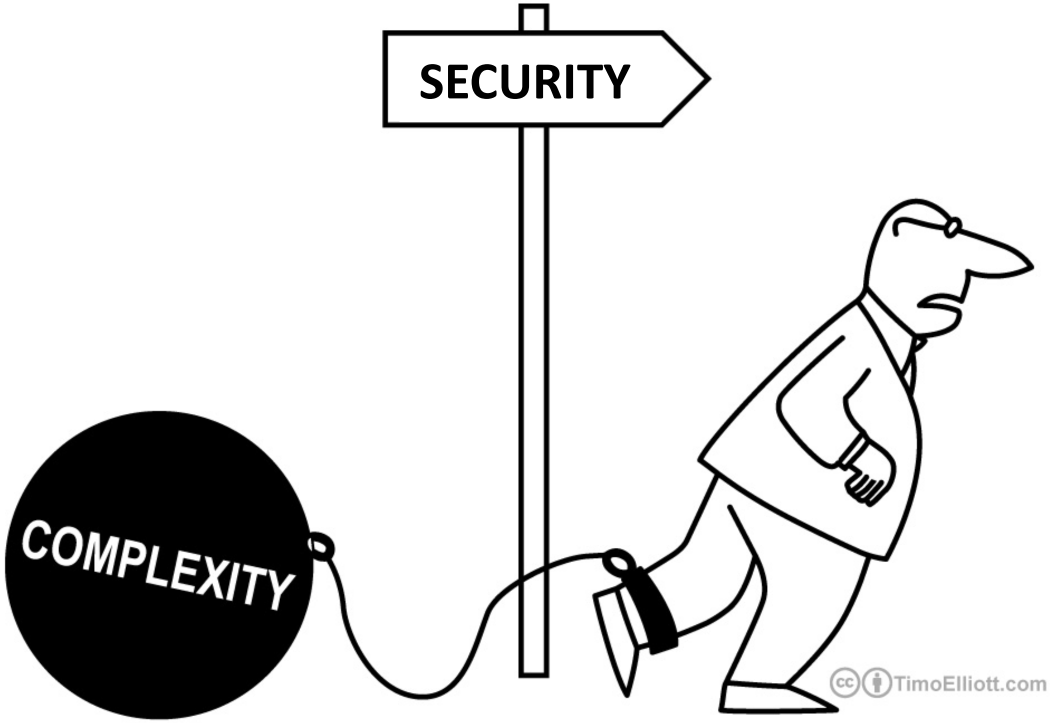
Security and Complexity

- Objective: To stimulate debate – you may disagree
- Key question: WHERE is the complexity? In the system, or in the security control (SC)?



Security and Complexity

- Complexity in the system
  - This is generally seen as BAD for security – complexity means too many factors to consider leading to things overlooked



Security and Complexity

- Complexity in the security control
  - This may be good or bad for security – depends on the security control – examples
  - If complexity is good for security, consider:
    - Is complexity necessary for security?
    - Is complexity sufficient for security?

Security and Complexity

- Complexity in the security control that is BAD for security:
  - Example: PKI
    - The average person finds it too difficult to understand, and therefore turn away from using it. If PKI is not used, it is BAD for security

Security and Complexity

- Complexity in the security control that is GOOD for security:
  - Example: Passwords
  - Example: Encryption
- Consider again passwords
  - Is complexity necessary for good passwords? – Yes
  - Is complexity sufficient for good (100% effective) passwords? – No
- In general, is complexity necessary for an effective security control – it depends on the control (e.g., role-based AC). Is complexity sufficient for an effective security control – No.

Security and Complexity

What do YOU think?

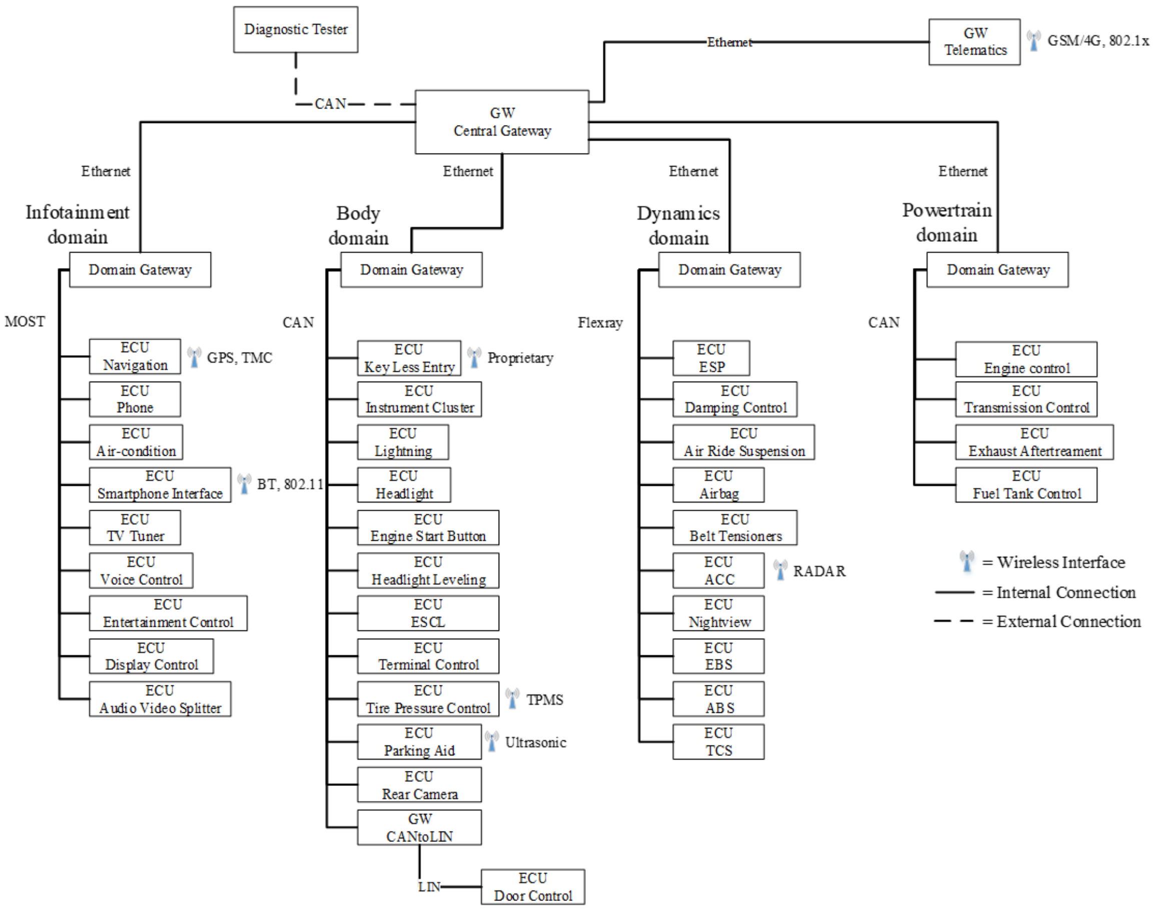
Security Mechanisms for Cyber-Physical Systems (Automotive needs)

Prof. Reiner Kriesten
Institut für Energieeffiziente Mobilität (IEEM)
Hochschule Karlsruhe – Technik und Wirtschaft (HsKA)

Acutal cars - complexity

…more than 100 Million lines of code highly distributed…

IEEM Referenzarchitektur



Diagnostic Tester
CAN
GW Central Gateway
Ethernet
GW Telematics
GSM/4G, 802.1x

Ethernet
Infotainment domain
Domain Gateway
MOST
ECU Navigation — GPS, TMC
ECU Phone
ECU Air-condition
ECU Smartphone Interface — BT, 802.11
ECU TV Tuner
ECU Voice Control
ECU Entertainment Control
ECU Display Control
ECU Audio Video Splitter

Ethernet
Body domain
Domain Gateway
CAN
ECU Key Less Entry — Proprietary
ECU Instrument Cluster
ECU Lightning
ECU Headlight
ECU Engine Start Button
ECU Headlight Leveling
ECU ESCL
ECU Terminal Control
ECU Tire Pressure Control — TPMS
ECU Parking Aid — Ultrasonic
ECU Rear Camera
GW CANtoLIN
LIN
ECU Door Control

Ethernet
Dynamics domain
Domain Gateway
Flexray
ECU ESP
ECU Damping Control
ECU Air Ride Suspension
ECU Airbag
ECU Belt Tensioners
ECU ACC — RADAR
ECU Nightview
ECU EBS
ECU ABS
ECU TCS

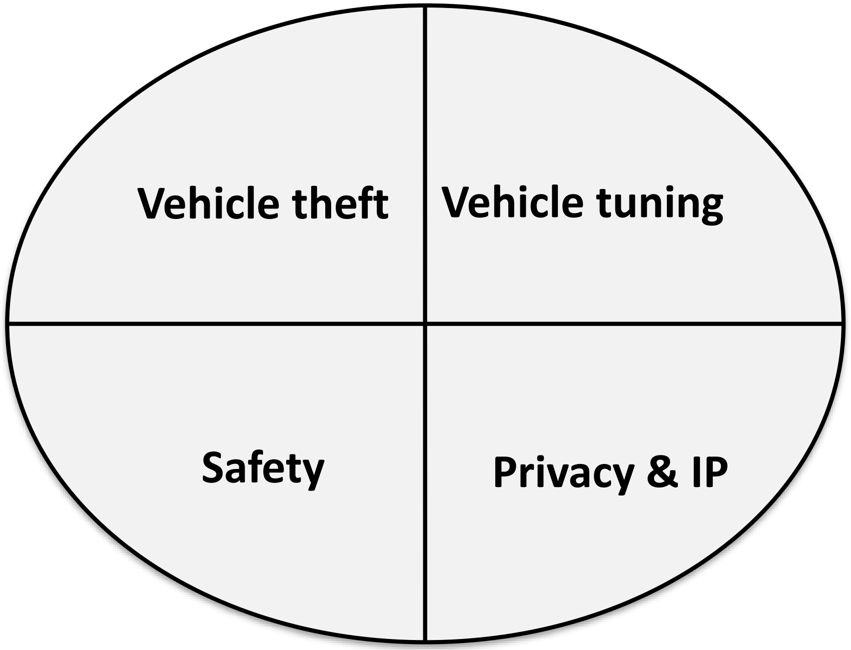
Ethernet
Powertrain domain
Domain Gateway
CAN
ECU Engine control
ECU Transmission Control
ECU Exhaust Aftertreament
ECU Fuel Tank Control

= Wireless Interface
= Internal Connection
= External Connection

Viewpoint Attacker (IT)

Assets IT-Hacking:

- Confidentiality:: Privacy (individual / scalable)
- Confidentiality:: Intellectual Property: Leackage of secret information, e.g. strategies, technical details,..
- Integrity, Availability: e.g. DDoS-Angriffe, Manipulation attacks



Vehicle theft

Vehicle tuning

Safety

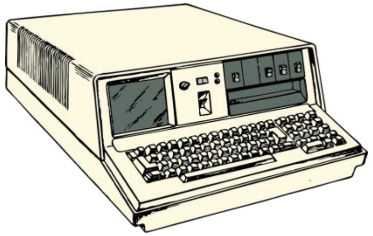
Privacy & IP

Relevanz Sicht Fahrzeugindustrie:

- Safety: high due to standards
- Privacy: rising importance
- IP: differs
- Theft / -tuning: individually not important, but fleet analysis, e.g. via key Management

Differences viewpoint Security IT versus CPS-automotive

- Hazard and Risk Analysis:
  Integration von Safety (ISO 26262)

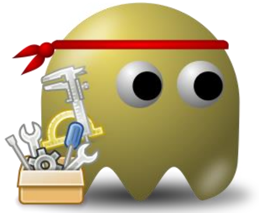


- Hardware: no exchange

- Vulnerability databases

- Physical access and tamper proof
  versus costs

- Availability Experts Embedded Security



IARIA **Securware 2019, Nice, France**

Simplified human device interaction – Striving for zero touch

Steffen Fries, Siemens AG, Germany

October 28th, 2019

security has to be suitable for the addressed environment

Awareness and Acceptance

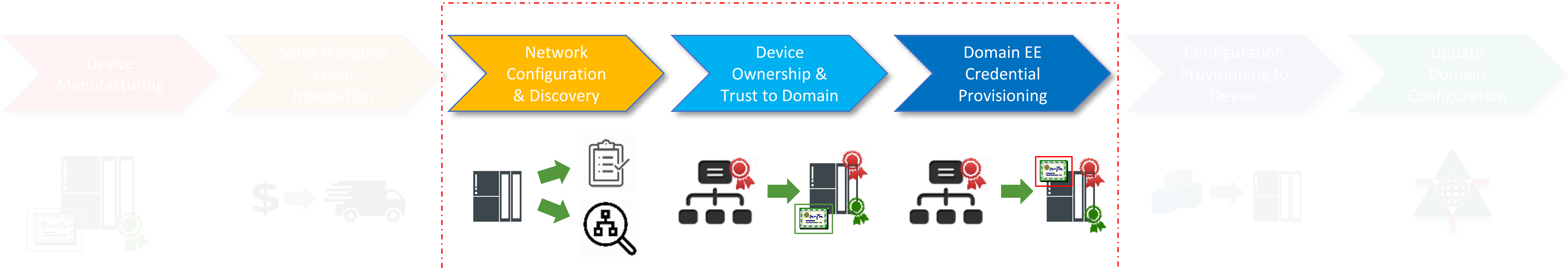
Security is not just a technical solution, which can be incorporated transparently. We need to consider how humans interact with it.

This needs, especially for automation environments, actions for:

- awareness trainings
- help people to understand security measures and processes
- provide user friendly interfaces and processes

Technology can be leveraged to ease the interactions with security functionality on devices. An example is provided for bulk onboarding of IoT devices (see next slides)

mutual trust establishment during the onboarding of devices



Device Manufacturing

Manufacturer provides *device* with *identity* and ideally authentication information.

Sales & Supply Chain Integration

Device is sold and shipped *to custome*r.

Siemens-internal sales systems contain customer information, or customer receives (digital) document from Siemens containing device information, e.g., device ID.

Network Configuration & Discovery

Device obtains connectivity in customer (network) domain, possibly with network access control.

Device Ownership & Trust to Domain

Device *authenticates itself as Siemens device*.

Customer domain claims device and *proofs possession of this device*.

Provision *domain trust anchor to device* (e.g. domain CA certificate) .

Domain EE Credential Provisioning

Device is provisioned with *domain specific end-entity credentials*.

Configuration Provisioning to Device

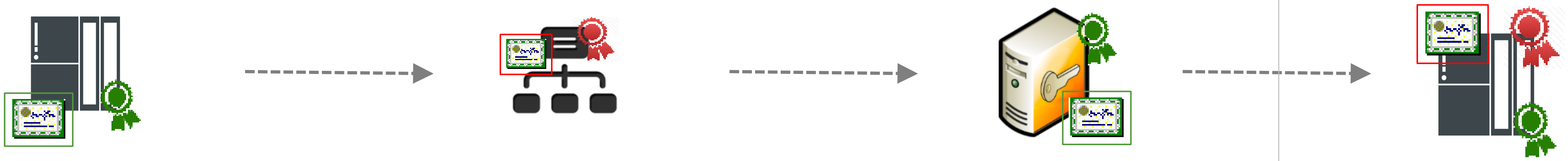
Device is provisioned *with information specific for the local domain*, e.g. configuration data, communication endpoints, etc.

Update Domain Configuration

Network is updated with device specific information to enable communication flow, e.g. firewalls, Cloud IoT service, etc.

Mutually trustworthy establishment of operational security credentials (LDevID) based on manufacturer provided security credentials (IDevID). This is typically done in these phases of **Secure Zero Touch Onboarding**. Technically, this is supported e.g., by the IETF work on Bootstrapping Remote Secure Key Infrastructures (BRSKI) to allow for automated onboarding.

how does the zero touch trick in IETF BRSKI work?



device from manufacturer has:

- a manufacturer issued certificate (and corresponding private key)
- manufacturers root certificate

voucher request

- Device signs request using manufacturer issued credential
- Device validates response using manufacturer root certificate and installs target domain certificate as additional trust anchor.

target network, features:

- operator issued certificates (and the corresponding private key) for entities
- operator root certificate

manufacturer services to:

- Support trust establishment of device to domain by signing the target domain certificate in a voucher response

voucher response

results in :

- adopting new root of trust from the target network operator on device side based on voucher response
- Continue with certificate enrollment of operator issued certificate provided to device to become trusted part of the network

End entity (EE) certificates from Manufacturer or traget domain

Private Key End Entity (EE)

Private Key Manufacturer

Root certificates from: Manufacturer, target domain

conclusion

- analyze your expected target environment to know how users interact with devices

- derive security requirements (follow security-by-design)

- match existing technologies to be applicable or alternatively develop new technologies for the intended operational environment to enable easy interaction with security functions