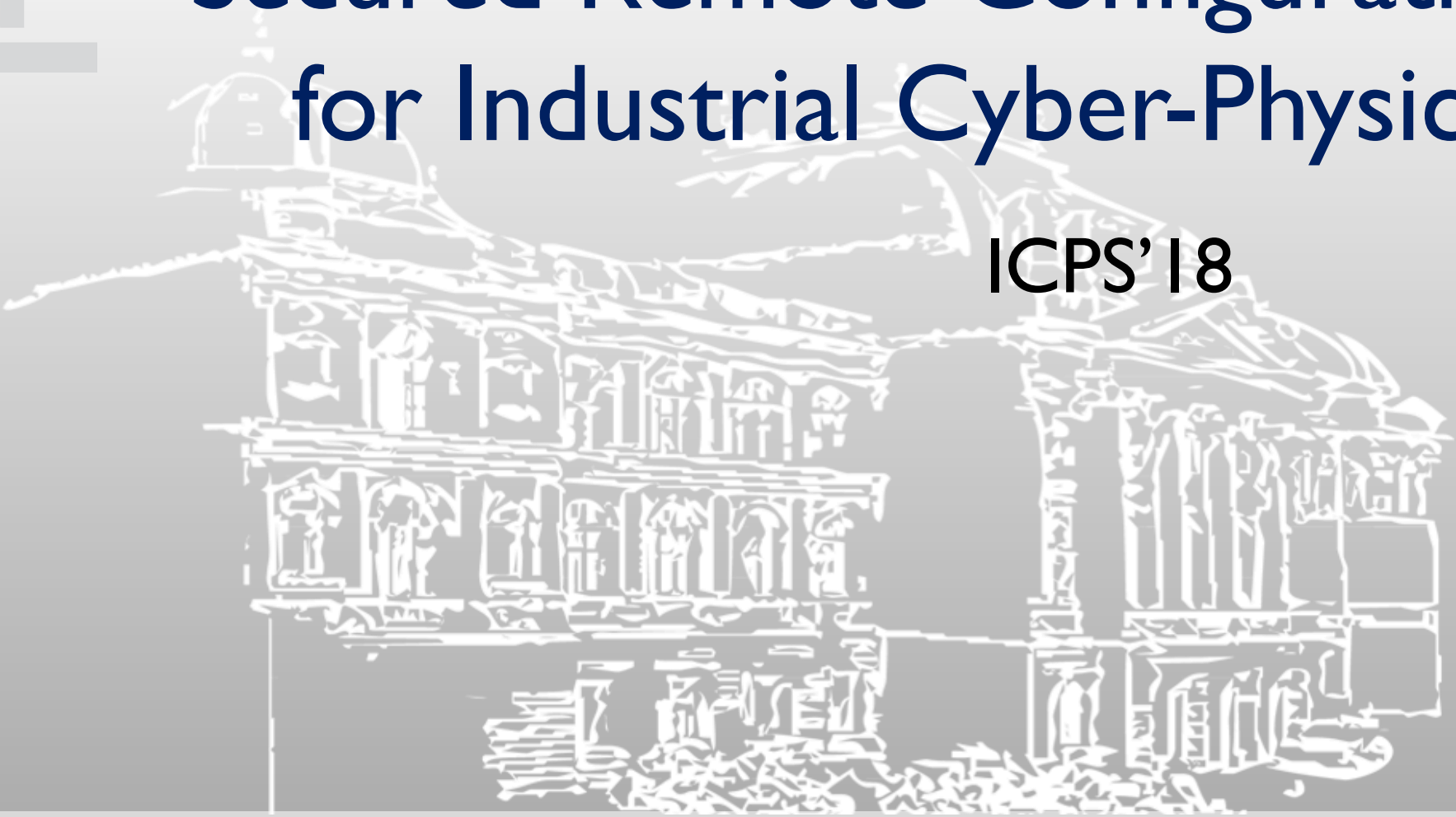
Secured Remote Configuration Approach for Industrial Cyber-Physical Systems

ICPS'18



Thomas Ulz, Graz UT
(thomas.ulz@tugraz.at)
Thomas Pieber, Graz UT
Christian Steger, Graz UT
Sarah Haas, Infineon Austria
Rainer Matischek, Infineon Austria

Outline

1. Introduction
   1. Motivation
   2. System Model
2. Secured Remote Configuration
   1. Connection Concept
   2. Security Concept
3. Threat Analysis
4. Conclusion

Introduction – Motivation

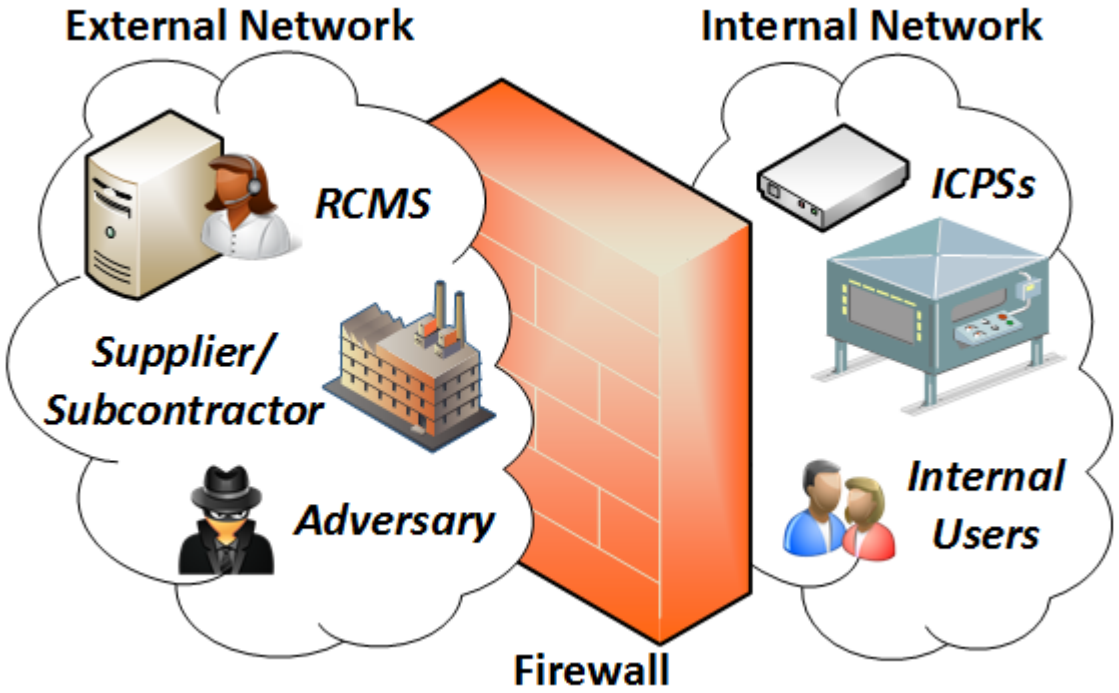
- ICPS represent challenging security aspects compared to traditional IT systems and the Internet of Things (IoT)
  - If used in industrial processes: availability most important aspect
  - Need to be operated continously
  - ICPS interact with the physical world
    - Attacks can cause serious damage to physical entities
- However, security related issues known from other domains exist
  - Default configurations such as username and password combinations lead to severe attacks where a device is taken over by the adversary

Introduction – Motivation

- Local configuration updates can be applied by service technicians or the ICPS user itself
  - Often inconvenient
- Nowadays, many ICPS can be remotely configured
  - For instance via a cloud-based remote configuration management system (RCMS) provided by the manufacturer
- Drawbacks:
  - Remote access to ICPS needs to be granted
    - Configuration interface exposed to network; accidental or deliberate misuse
    - Also, administrative overhead if remote access is granted on demand

Introduction – System Model

- „Internal“ network separated from „external“ network
- Internal: ICPSs, internal users
- External:
  - Other sites, suppliers, subcontractors
  - Remote configuration management system (RCMS)
  - Also: Adversaries



Outline

1. Introduction
   1. Motivation
   2. System Model
2. Secured Remote Configuration
   1. Connection Concept
   2. Security Concept
3. Threat Analysis
4. Conclusion

Secured Remote Configuration – Requirements

- Allow RCMS to access ICPSs
  - Without granting permanent remote access
  - Also without entailing administrative overhead of temporarily granted remote access rights
  - Easy to monitor for security-aware personnel

- Thus, we propose to use dedicated configuration update hardware
  - *Temporarily* attached to ICPS that should be remotely configured

Secured Remote Configuration

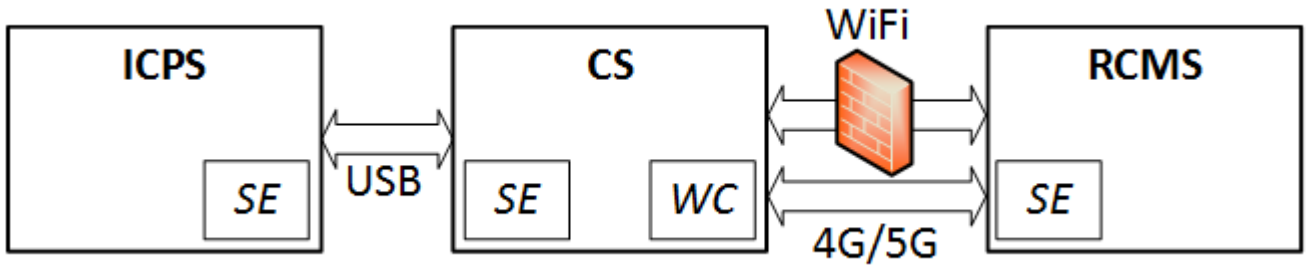
- Advantages of such an approach are
  - During normal operation, configuration interface is not attached
    - Attacks targeting the configuration interface are not possible most of the time
  - Straightforward to initiate, monitor, and control ongoing configuration updates
    - By local personnel; it requires no knowledge to attach the interface; monitoring is easy
  - Overhead due to remote configurations is limited
    - Only a small number of so-called configuration sticks (CS) need to be administrated

- Disadvantage: manually attaching the CS, but this is more of an advantage

Secured Remote Configuration

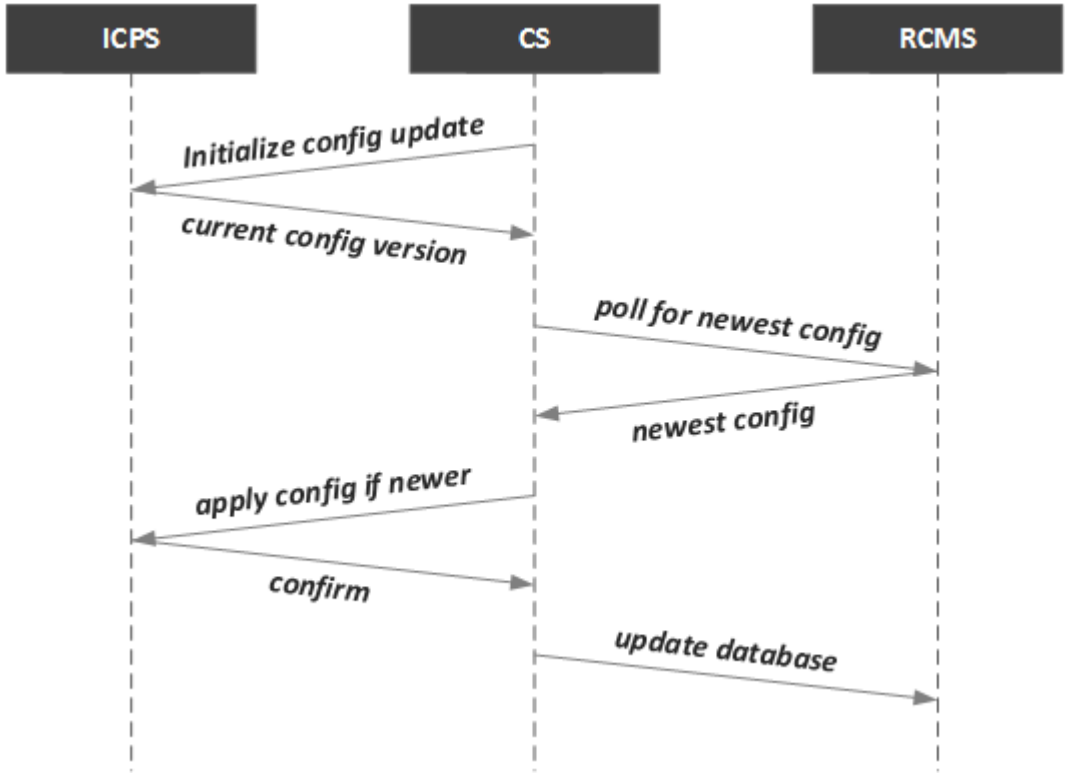
- We propose two wireless communication (WC) technologies for the CS:
  - WiFi: infrastructure needed, also needs to be administrated, BUT: higher data rates
  - 4G/5G: zero administrative overhead, BUT usually slower compared to WiFi

- For security reasons: Secure Element (SE) included in all three entities
  - More on security in a minute



Secured Remote Configuration – Connection Concept

- General process of configuraiton updates in our approach
  - Update is initiated by the CS
  - RCMS is pooled for new update
    - Can be prepared at any time before actual update process, so „offline“
  - ICPS applies config is new
  - CS reports successful update to RCMS



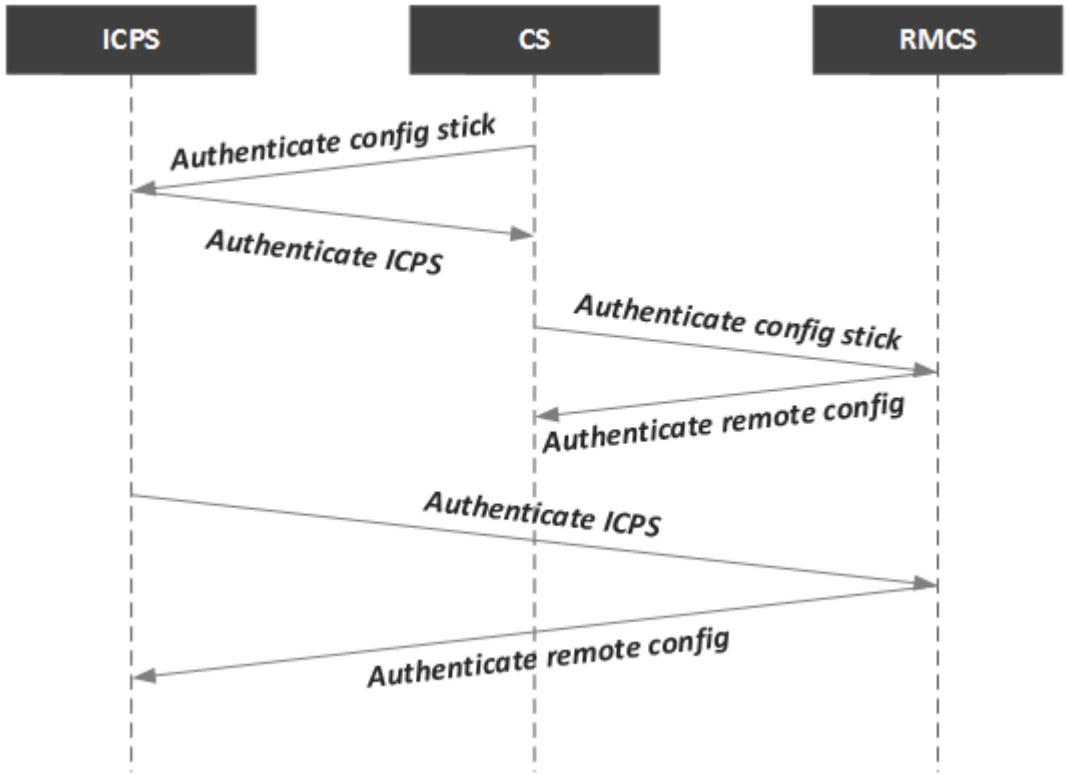
Secured Remote Configuration – Security Concept

- Two critical steps
  - 3-Way mutual authentication
  - Secured data transfer channel

- All security related operations in SE
  - Dedicated hardware security
  - Tamper resistant and security certified
    - Information cannot be extrated by physical attacks

Security Concept – 3-Way Mutual Authentication

- Authenticity of all three involved entities must be ensured
- Method: for instance certificates
- After this process is finished
  - Trust relationship between all three involved entities



Security Concept – Secured Data Channel

- Since both ICPS and RCMS trust the CS, it can act as a gateway
- Two encrypted connections are established
  - TLS is used between RCMS and CS
  - Authenticated Encryption (AE) is used between ICPS and CS
- Since the CS does not need to read the configuration data
  - It can be encrypted at the RCMS and decrypted by the ICPS
  - End-to-end encryption

Security Concept – Secure Element

- To increase security, we propose to use the SE for three tasks
  - Certificates and private keys used for mutual authentication authentication are stored in the SE‘s protected memory.
  - Authentication of entities is performed in the SE‘s secured execution envirionment
  - Session keys for encrypting data are generated by the SE and stored in ist protected storage. Also, encryption and decryption using these keys are performed by the SE.

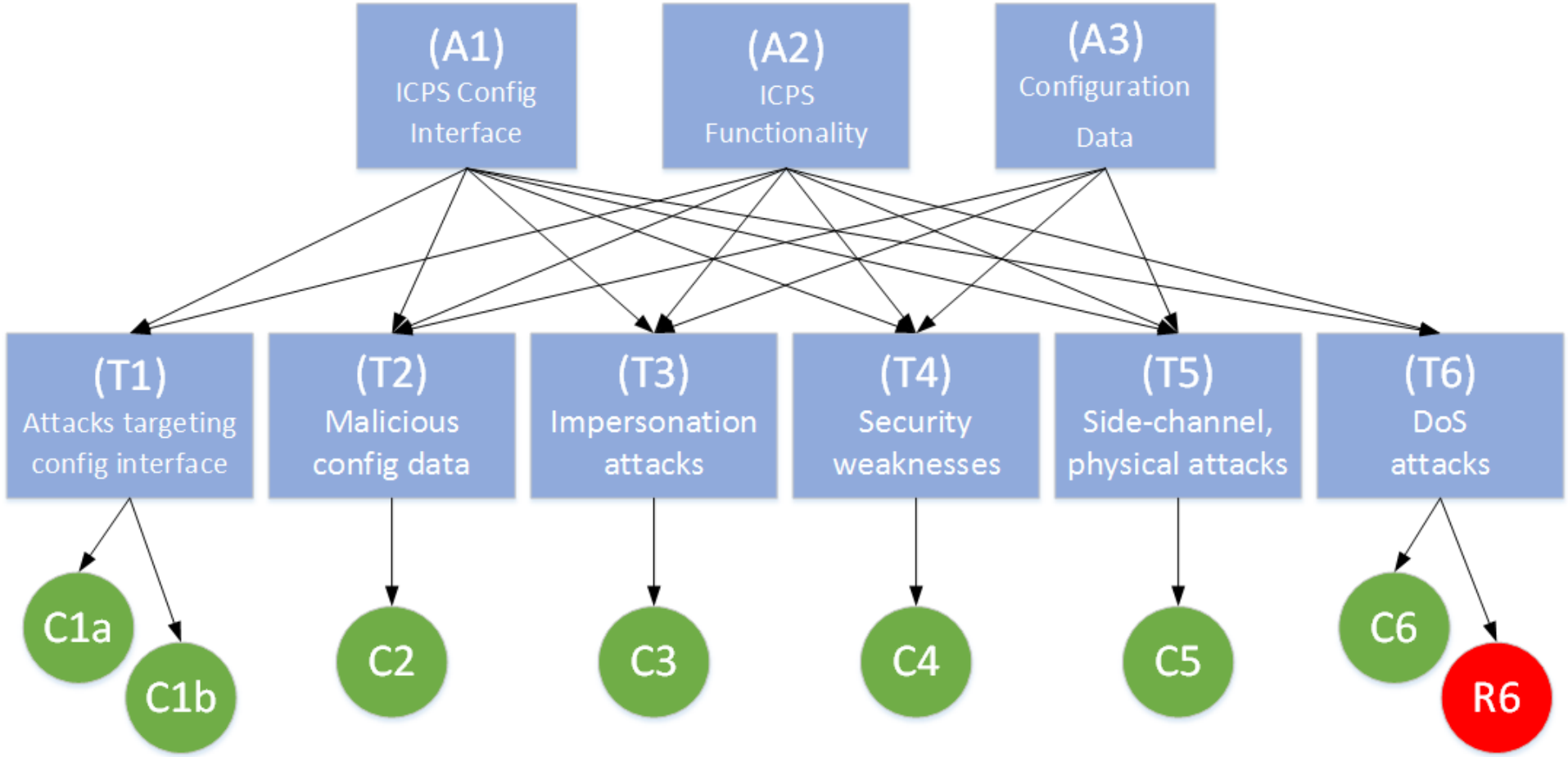
Outline

1. Introduction
   1. Motivation
   2. System Model
2. Secured Remote Configuration
   1. Connection Concept
   2. Security Concept
3. Threat Analysis
4. Conclusion

Evaluation – Threat Analysis

- For evaluating the provided security level
  - 7 entities (ICPS, CS, RCMS, ICPS manufacturer, CS manufacturer, adversary)
  - 3 assets that need to be protected (ICPS configuration interface, functionality, configuration data)
  - 6 threats of which 5 are completely mitigated
  - 1 threat (denial of service attacks) can only be partially mitigated

Evaluation – Threat Analysis



Outline

1. Introduction
   1. Motivation
   2. System Model
2. Secured Remote Configuration
   1. Connection Concept
   2. Security Concept
3. Threat Analysis
4. Conclusion

Conclusion

- ICPS are either configured locally or remotely
- Existing remote configuration solutions have drawbacks
  - Security related and administrative overhead
- We propose to use dedicated configuration hardware
  - Configuration interface only attached temporarily
  - Thus, easy to monitor and manage
- Security concepts: 3-way mutual authentication and secure channel
- Threat analysis demonstrates that of 6 identified threats 5 can be completely mitigated while the 6th threat is partially mitigated

Acknowledgements

This project has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 692480. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Germany, Netherlands, Spain, Austria, Belgium, Slovakia.

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

IoSense is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2016 and April 2019. More information: https://iktderzukunft.at/en/

bmvit
Austrian Ministry
for Transport,
Innovation and Technology

Thank you! Any questions?

Thomas Ulz

thomas.ulz@tugraz.at

Institute for Technical Informatics
Hardware/Software-Codesign Group
Graz University of Technology