INNOVATIVE SECURE SENSOR NETWORKS AND MODEL-BASED ASSESSMENT TOOLS FOR INCREASED RESILIENCE OF WATER INFRASTRUCTURES

SPONSORED BY THE

Federal Ministry of Education and Research

Cyber Security

Impact and Risk Analysis of the IT Infrastructure for Water Utilities

David Meier

French-German project funded by ANR/BMBF

Critical Infrastructure Protection Call

PICS 2014 – Final meeting

Dresden, the 26th June 2018

Overview

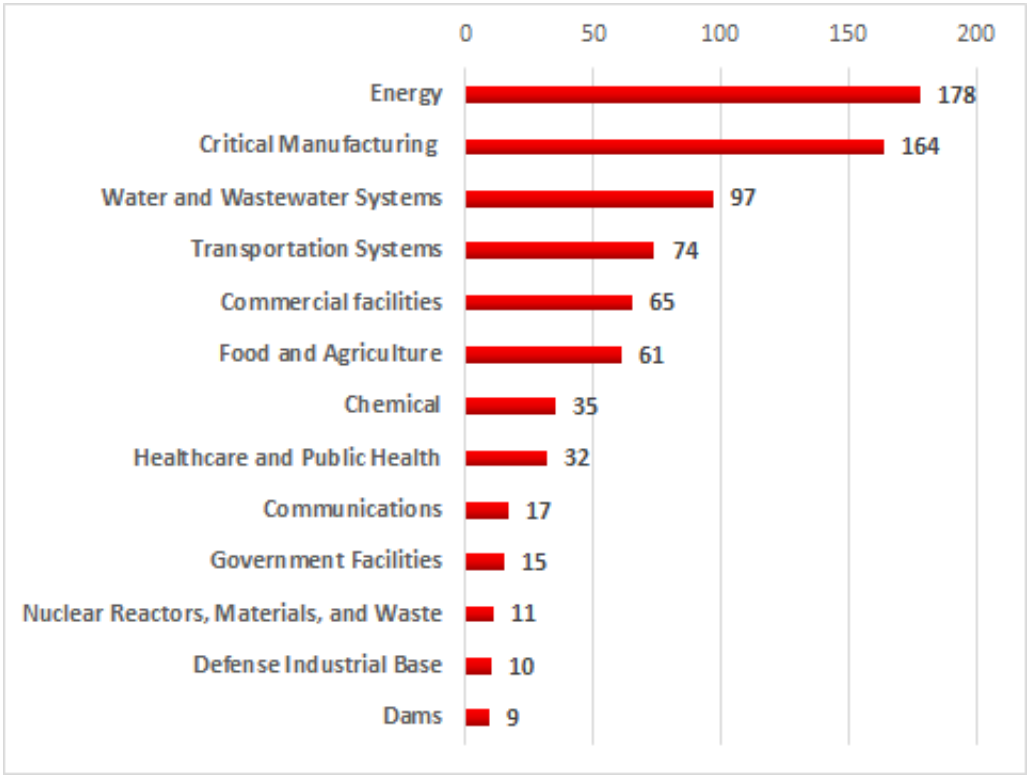
- Cyber Security Approach
  - Building a Cyber Security Management System
- Risk analysis
- Risk addressing
- Results and Outlook

SPONSORED BY THE
Federal Ministry of Education and Research

Motivation

- Threat landscape is increasing
- All industrial areas are affected
- High impact potential
- Safety implications

Number of vulnerable products (ICS-Cert 2017)



https://ics-cert.kaspersky.com/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017/#_Toc509229750

SPONSORED BY THE
Federal Ministry of Education and Research

Cyber Security Approach

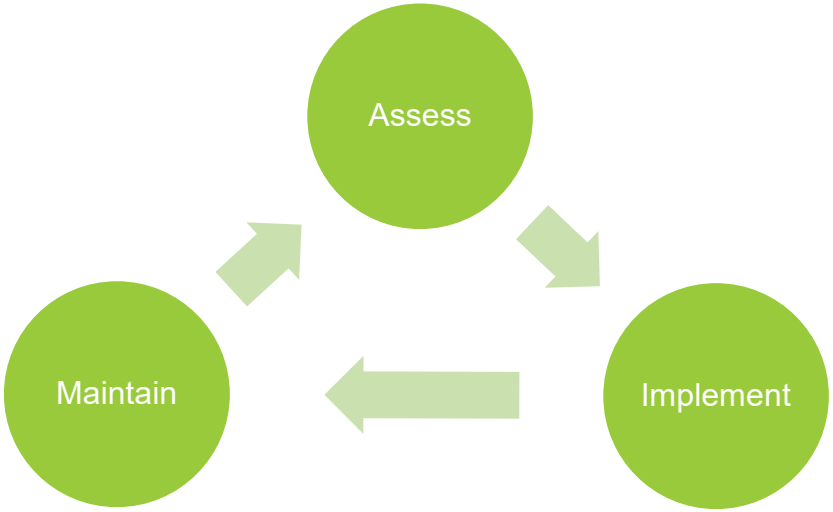
- Creation of a basic study of the communication architectures of BWB and EMS in respect to IT security
- Performing an IT security risk analysis
  - Incorporating scenarios from ResiWater WP1
- Providing recommendations for increased resilience against cyber threats

SPONSORED BY THE
Federal Ministry of Education and Research

Securing Industrial Control Systems

CYBER SECURITY MANAGEMENT SYSTEM

- Risk analysis is the building block for a CSMS
  - „Cyber security management system“
- Following industrial security standard IEC 62443
  - Standard for Industrial Communication System (ICS) security
  - Establishing security for industrial automation and control systems



SPONSORED BY THE
Federal Ministry of Education and Research

Securing Industrial Control Systems

CYBER SECURITY MANAGEMENT SYSTEM

- Consisting of three main parts:
  1. Risk analysis (risk identification, classification and assessment)
  2. Risk addressing (security policies, awareness, countermeasures)
  3. Monitoring and improvement

SPONSORED BY THE
Federal Ministry of Education and Research

Cyber Security Risk

CYBER SECURITY MANAGEMENT SYSTEM

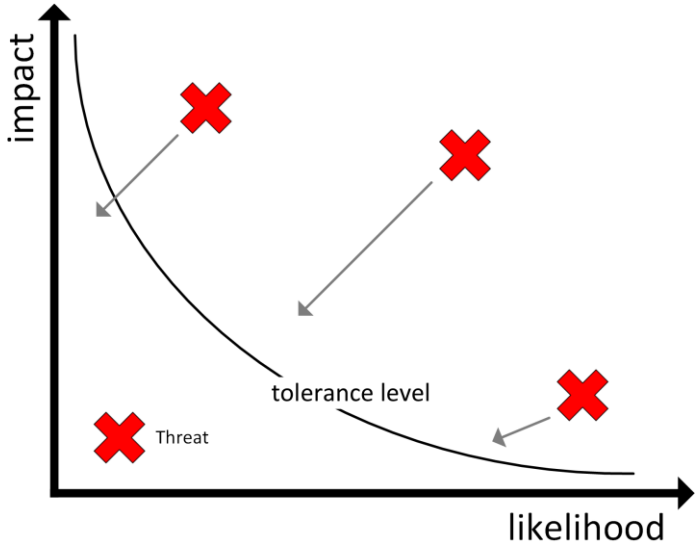
- Based on simple risk definition
  - Risk = Threat x Vulnerability x Consequence
- Threat
  - likelihood that a threat against an asset is realized
- Vulnerability
  - how likely it is that a vulnerability can be exploited
- Consequences
  - the negative impact on the organization after a successful attack

SPONSORED BY THE
Federal Ministry of Education and Research

Cyber Security Risk

CYBER SECURITY MANAGEMENT SYSTEM

- Focus in risk analysis
  - Risk identification (which risks/threats exist?)
  - Risk classification (properties of risks/threats)



SPONSORED BY THE
Federal Ministry
of Education
and Research

Risk Analysis

RISK IDENTIFICATION, CLASSIFICATION AND ASSESSMENT

- Risk analysis incorporating results from WP1 (use cases)
  - Analysed per operator

SPONSORED BY THE
Federal Ministry of Education and Research

Risk Analysis

IDENTIFIED RISK AREAS

- Identified crucial assets and systems components affected by scenarios

- PLCs and programming stations
  - Can be manipulated (different process logic, false process data)

- Control authorization and handover concept
  - Control safeguarding crucial to failover concepts

- System and sensor monitoring
  - Manipulated data can lead to bad decisions

- Network design
  - Decreases vulnerability and increases resilience

SPONSORED BY THE
Federal Ministry of Education and Research

Risk Analysis
IN RESIWATER

- Performing interviews with key staff
  - BWB (August 2016)
  - EMS (September 2016)

- Example questions:
  - How is the system structured?
  - What IT security topics have already been addressed?
  - What systems are in use, how are they secured?
  - How are IT security procedures implemented?

- Performing analysis of results
  - Benefitting from differences between BWB and EMS
  - Focus on identified risk areas

SPONSORED BY THE
Federal Ministry of Education and Research

Securing Industrial Control Systems

CYBER SECURITY MANAGEMENT SYSTEM

- In order to reduce risk, it needs to be addressed
- Concentrate on policies, countermeasures and implementation details

SPONSORED BY THE
Federal Ministry of Education and Research

Risk Addressing

SECURITY POLICY, ORGANIZATION AND AWARENESS

- CSMS Scope
  - Organization has to decide what will be covered by CSMS
- Organize for security
  - Responsible staff has to be named and process needs to established
- Staff training and security awareness
  - Includes sub-contractors
- Business continuity plan
  - Disruption recovery plans, includes testing
- Security policies and procedures
  - Define security program, set risk acceptance levels

SPONSORED BY THE
Federal Ministry of Education and Research

Risk Addressing

SECURITY COUNTERMEASURES

- Personnel security
  - Security policy, screening, segregates duties and responsibilities
- Physical and environmental security
  - Physical protection, including against environment
- Network segmentation
  - Separate network elements, usage of conduits, block non-essential communication
- Access control
  - Account administration
    - Assign accounts to individual entities, review state
  - Authentication
    - Authenticate all users, log and review
  - Authorization
    - Role-based access control, who is granted privileges?

SPONSORED BY THE
Federal Ministry of Education and Research

Risk Addressing

IMPLEMENTATION

- Risk management and implementation
  - Manage risks at accepted level, decide which countermeasures to use („common set of countermeasures“)
- System development and maintenance
  - Maintain security status while evolving assets (e.g. introduction of new components, changes to the system)
- Information and document management
  - Ensure long-term records, classify information assets
- Incident planning and response
  - Prepare reaction to incidents (includes detection of incidents)
  - Practice incident response
  - Address discovered issues

SPONSORED BY THE
Federal Ministry of Education and Research

Securing Industrial Control Systems

CYBER SECURITY MANAGEMENT SYSTEM

- Recommendations for addressing risk areas
- Based on risk analysis results and available controls

SPONSORED BY THE
Federal Ministry of Education and Research

Recommendations

BASED ON RISK ANALYSIS

- System hardening
  - Limit systems to only required functionality
- Secure network design, defence in depth
  - BWB analysis result demonstrates effectiveness of thorough network security design
- Deployment of secure technology
  - Reduce vulnerabilities
- Policies
  - Concrete rules are needed
  - Orientation for staff
- Organisation wide security concept
  - Combine corporate and operational efforts
- Raising awareness
  - Awareness of personnel is the key to success

SPONSORED BY THE
Federal Ministry of Education and Research

Conclusion and Outlook

- Cyber Security threat landscape is growing
  - Needs to be addressed for increased resilience
- Cyber Security is a process
  - Constant monitoring and improvement needed

SPONSORED BY THE
Federal Ministry of Education and Research

Thank you for your attention
Any questions?

www.resiwater.eu

SPONSORED BY THE
Federal Ministry of Education and Research