Honeywell Industrial Cyber Security

AIChE conference – Cyber Security Engineering

April, 2015

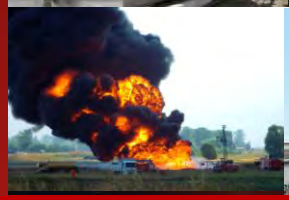
Honeywell

Global Multi-Industry Topic

Some level 0 cyber security incidents

- Oil & Gas
- Power
- Steel factory






Some examples

Oil & Gas

- 2008
- Turkey
- Pipeline rupture / explosion
- Entered control network through the camera systems
- Hydrological shock
- Possible cause:
  - Valve travel time

Power

- 2013
- UK
- Wind turbine blade damage
- Entered the system through a wireless connection
- Mechanical stress
- Possible cause:
  - Compromised pitch control

Steel factory

- 2014
- Germany
- Blast furnace damage
- Entered the control system through corporate network
- Thermal shock
- Possible cause:
  - Uncontrolled cool down

Multifaceted Topic

Some other cyber security issues

- Havex, a Trojan horse
- Supply chain attacks
- Ransomware

Some examples

Havex, a Trojan horse

- 2014.
- Compromised vendor software
- Targets OPC servers
- Spyware, collects control information and returns this to a control & command server on the Internet

Supply chain attacks

- 2015
- Network or computer hardware delivered with malware installed on it already
- Sometimes propagates at firmware level out of sight antivirus
- Emerging threat because build up of cyber war capabilities

Ransomware

- 2014
- Restricts access to computer systems, e.g. using encryption
- Demands a ransom for getting the decryption key
- Very dangerous because an infection halts the control system immediately

Cyber security engineering

Two kinds of cyber security engineering

- Security plumbing
- Security architecture building

Cyber security engineering is a team effort

Security plumbing

- Applying point solutions
- Tactical goals
- Atomistic approach
- IT centric
- Add-on cyber security
- Not recognizing ICS cyber security as a specialized skill set
- Low resilience against targeted cyber security attacks

Security architecture building

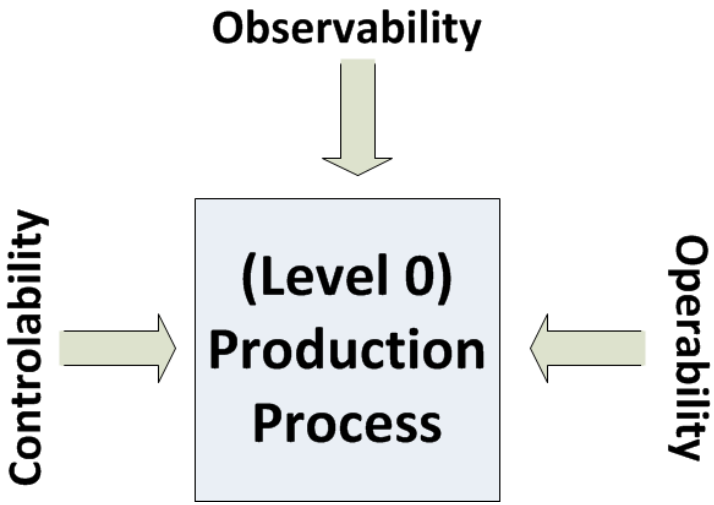
- Applying a framework within security complexity is managed
- Risk aware strategic goals
- Holistic approach
- IT, OT and operations centric
- Integrated cyber security
- Specialist multi-disciplinary teams of cyber security professionals
- High resilience against ICS specific targeted and generic type of attacks

Cyber security objectives

Multiple consequence

- Damage to equipment
- Production loss
- Compliance violations

Security objectives for the production system



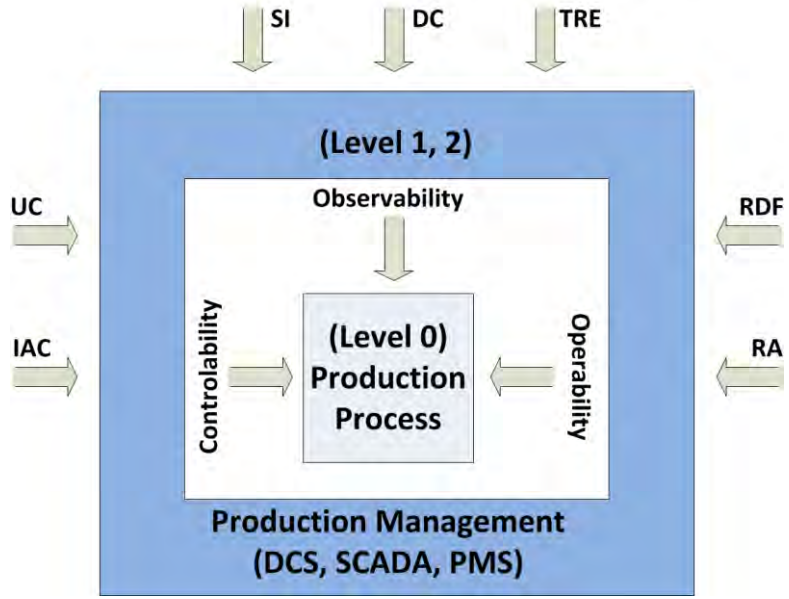
- **Controlability, e.g.**
  - Control direction (Direct, reverse)
  - Control mode (COM, CASC, AUTO, MAN)
  - Control parameters (P, I, D)
- **Observability, e.g.**
  - Transmitter range
  - Thermo-couple characterization
- **Operability, e.g.**
  - Operating window integrity (Range, rates, alarms, alerts)
  - Safety control integrity, availability
  - Monitoring & diagnostic integrity, availability

Cyber security objectives

Production management environment

- DCS, SCADA, PMS
- Monitoring systems (Turbine, vibration), diagnostic systems
- Metering systems

Security objectives for the production management system



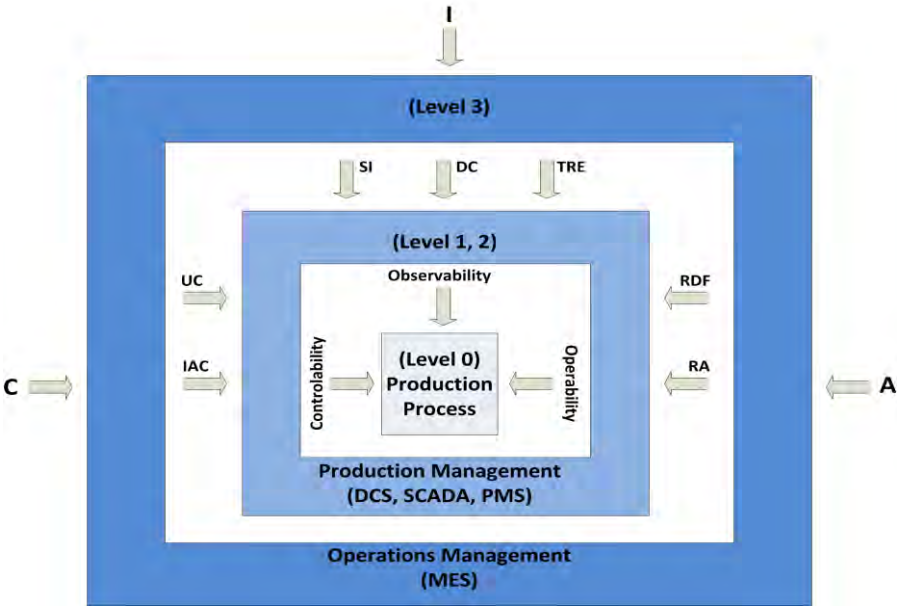
- **We need to control:**
  - Access / identification, authentication (IAC);
  - Use / authorizations (UC)
  - System integrity (SI)
  - Data confidentiality (DC)
  - Timely response to events (TRE)
  - Restrict the data flow (RDF)
  - Resource availability (RA)
- **The OT area, real-time performance required**

Cyber security objectives

Operations management environment

- Manufacturing Execution Systems (MES)
- Production quality management
- Production resource and inventory operations management

Security objectives for the operations management system



- **We need to control:**
  1) Integrity (I)
  2) Availability (A)
  3) Confidentiality (C)
- **Though no real-time performance, there is a tight integration with production management**
- **From a distance it might look like an IT environment but:**
  - Use of specific OT protocols
  - Impacts OT authorizations
  - Impacts OT data integrity

Cyber security projects

The EPC project lifecycle

- Cyber security engineering starts already at the conceptual design
- How later we add cyber security, the less effective it is
- Cyber security is in every phase of the system's lifecycle

Cyber security is a process, not a product

Security plumbing starts here

Conceptual design	Initial specifications	Front-end engineering	Procurement	Detailed engineering	Construction	Commissioning	Handover	Manage & monitor

Security architecture starts here

Cyber security projects

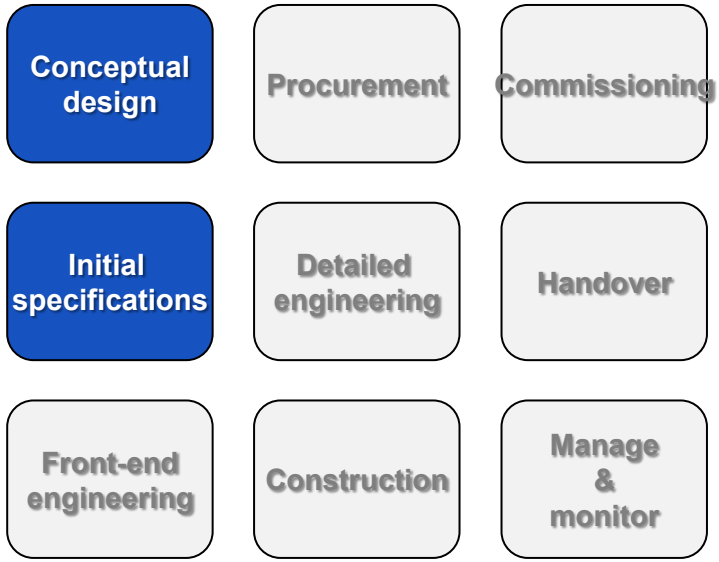
The EPC project lifecycle, strategy and concept

- Business drivers, including business assets, goals and objectives
- Which risk is acceptable, tolerable, and unacceptable?
- Which risk do we avoid, accept, share, or reduce with controls?

The design engine for cyber security is fueled with risk

Strategy and concept phase

- Business requirements
- Identify risk
- Select security strategies
- Specify control objectives
- Define trust relationships



Cyber security projects

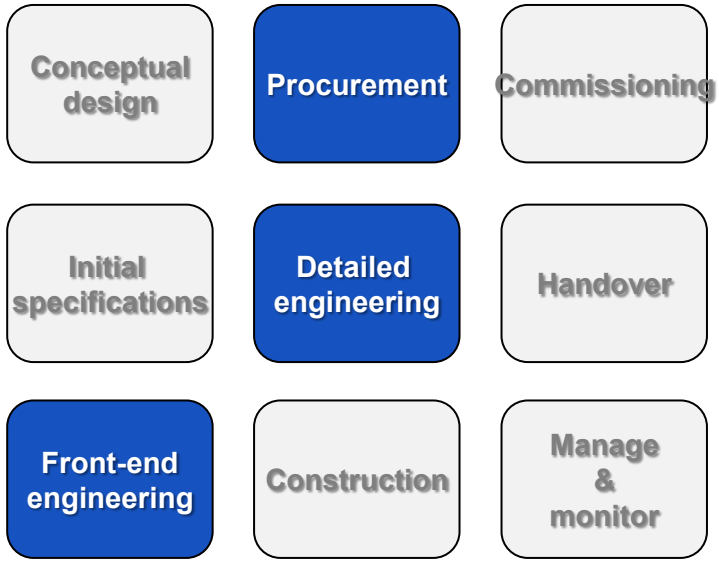
The EPC project lifecycle, the logical and physical design

- Input is an agreed and signed off conceptual security architecture
- Logical and physical architecture is developed
- Security standards will help you

Cyber security is a process, not a product

Design phase

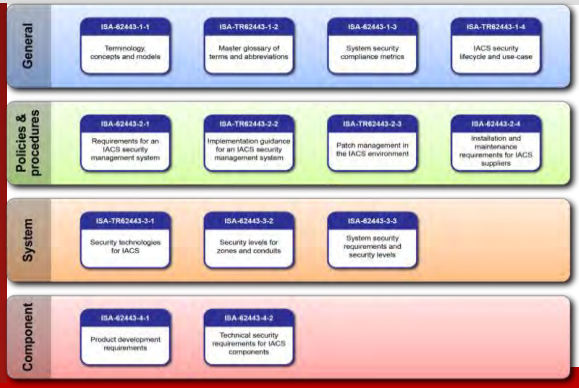
- Security policies and procedures
- List of security services
- Roles, responsibilities, and authorizations
- Security mechanisms to be implemented
- Platforms and network infrastructure
- Capacity and resilience planning
- Security products and tools
- Operational security architecture



Cyber security standards

Standards for industrial control systems

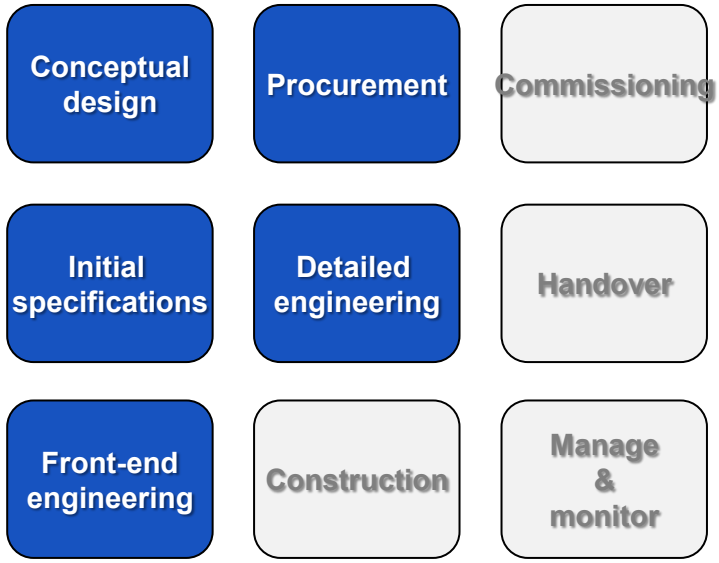
- Control equipment certification
- Security requirements for design
- Procurement language for specifying security requirements



Out of the box no ICS is amply secured, we need to add countermeasures

Standards for ICS

- IEC 62443.3.3 – technical security controls
- IEC 62443.2.2 – non-technical security controls
- IEC 62443.3.2 – cyber security risk assessment
- Cyber security procurement language for control systems (DHS)
- ISASecure EDSA certification for evaluation of embedded device security (process controllers, safety controllers, ..)
- But also IEC 61508 (Safety), API RP 584 (IOW)



Cyber security projects

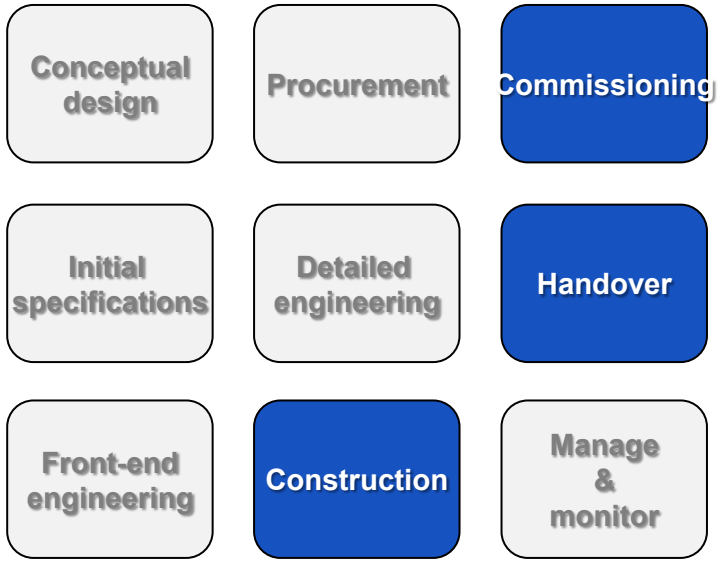
The EPC project lifecycle, implementation phase

- Implement the security mechanisms
- Verify security posture (pre-FAT, FAT)
- Validation (Penetration) testing during or after SAT

Don’t allow for “hidden” back doors and fixed security credentials

Implementation phase

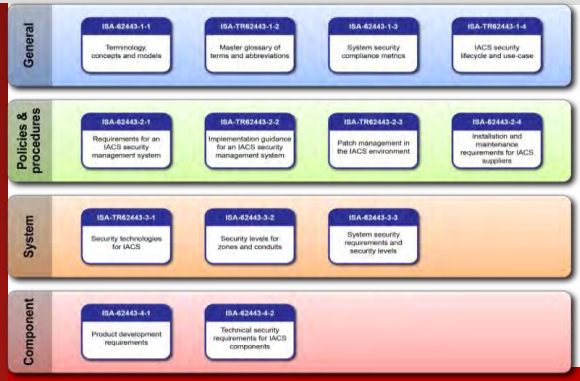
- Implement the security mechanisms
- Test plans
- Support documentation
- Training materials, training
- FAT (Verification testing: security settings, security patches, management procedures)
- SAT (Validation (penetration) testing)
- Change of security credentials



Cyber security standards

Standards for industrial control systems

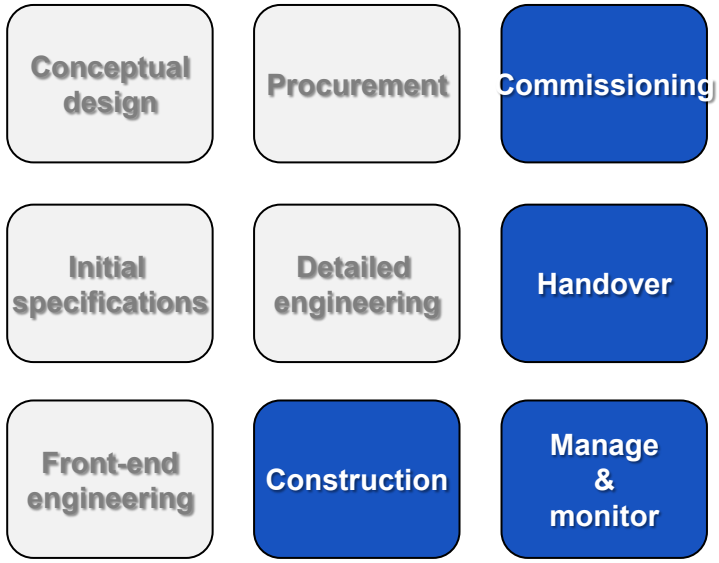
- How to organize the security patch process
- Project and service requirements
- Validation (Penetration) testing during or after SAT



Requirement for certified security leads

Standards for ICS

- IEC 62443.2.3 – Patch management
- IEC 62443.2.4 – Installation and maintenance requirements for ICS suppliers (WIB 3.0)



Best practices

Some basic rules

- Segment the network and control access to these segments
- Protect your computer nodes, antivirus, hardening
- Use strong passwords, change all manufacturer passwords

Critical infrastructure requires much more!

Cyber security has 5 dimensions

- Identification of risk
- Prevention of attack
- Detection of attack
- Response to attack
- Recovery from attack

Each of above elements are required, missing one will lead to vulnerabilities an attacker can exploit.

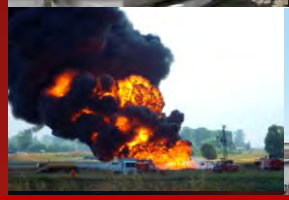
Network segmentation	End node protection	Policies & procedures
Access control	Antivirus	Roles & responsibilities
Security zones & conduits	White listing, Host IPS	Standards, Reference architecture

Summary

Summary

- Cyber security is part of all phases of the lifecycle, you can't ignore it. Prevent cyber security plumbing!
- Cyber security is a profession requiring education
- A cyber security attack may not have happened to you yet, but this is a matter of time. The problem rapidly increases.






Real incidents

- Pipeline ruptured
- Blast furnace damaged
- Wind turbine blade broken
- Environmental contamination
- Food quality spoiled
- Loss of intellectual property
- Rotating equipment damaged
- Turbine damaged
- Power grid breaker manipulation

Not only infrastructure

- Security zones need to be carefully chosen
- Protecting the conduit doesn't necessarily solve the problem
- Transmitters and valves are just as vulnerable today
- Authorizations within applications
- Separation of responsibilities
- Separation of control and safety

Phony security

- Make sure you solve the problem and don't throw away your money on bogus solutions
- Always keep risk in mind, the level of risk should determine your response to the risk. Under and over-protection frequently happens as result of security plumbing.
- If your security assessment never assessed the OT environment and was limited to infrastructure you have missed several important vulnerabilities.

Thank You

Honeywell