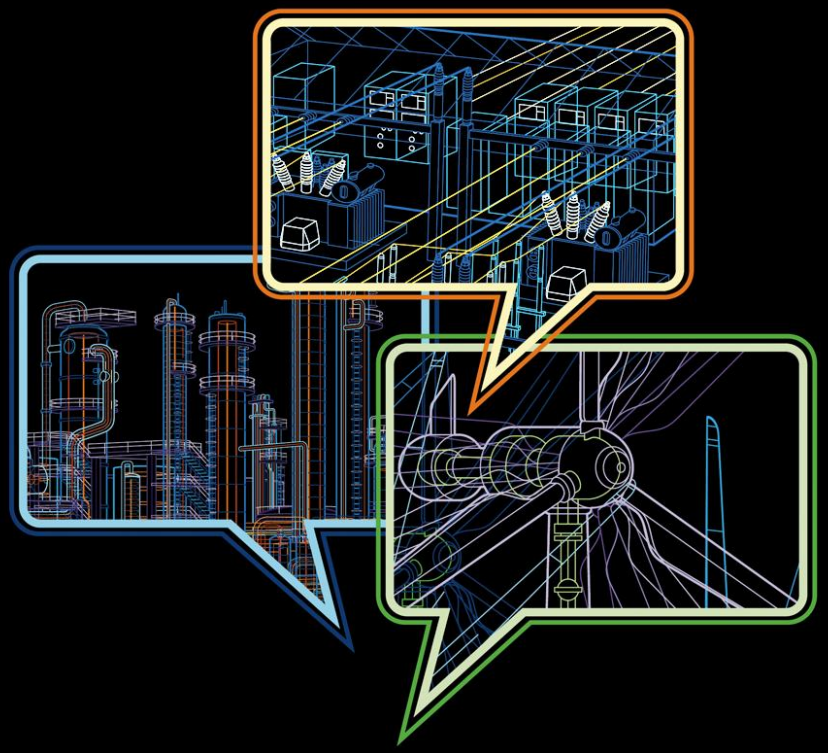


ABB Automation & Power World: April 18-21, 2011

WSE-107-1

Buying a pig in a poke? How to get the security you need!

WSE-107-1
Buying a pig in a poke? How to get the security you need!

- Speaker name: Ragnar Schierholz
- Speaker title: Principal Scientist
- Company name: ABB Corporate Research
- Location: Baden-Dättwil, Switzerland

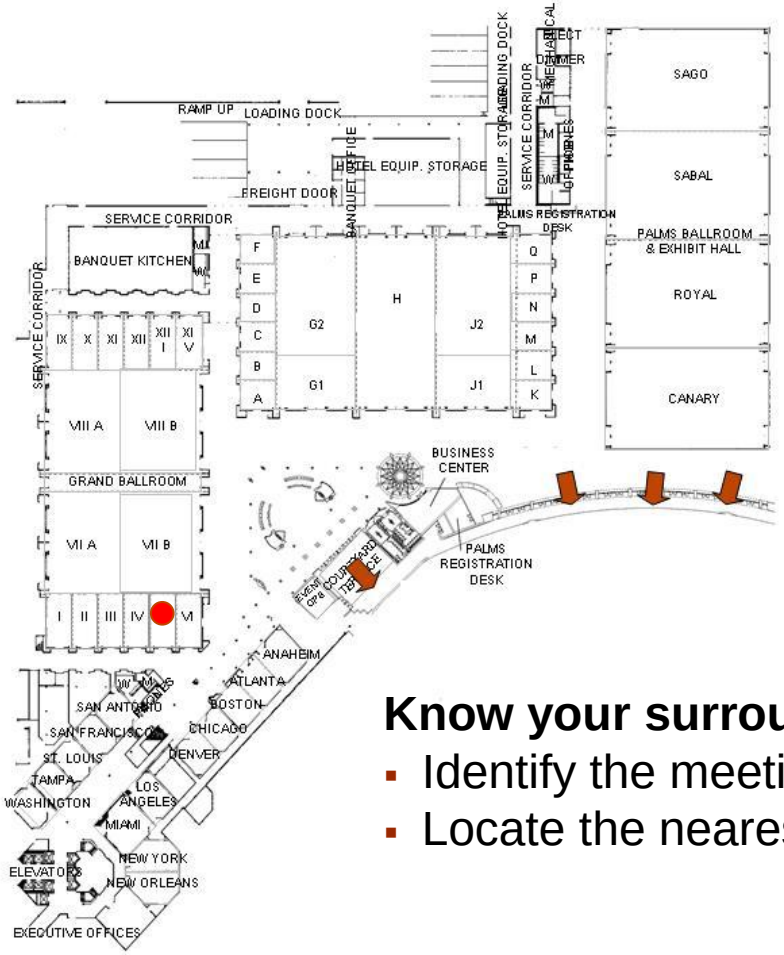
Co-presenter (if applicable)

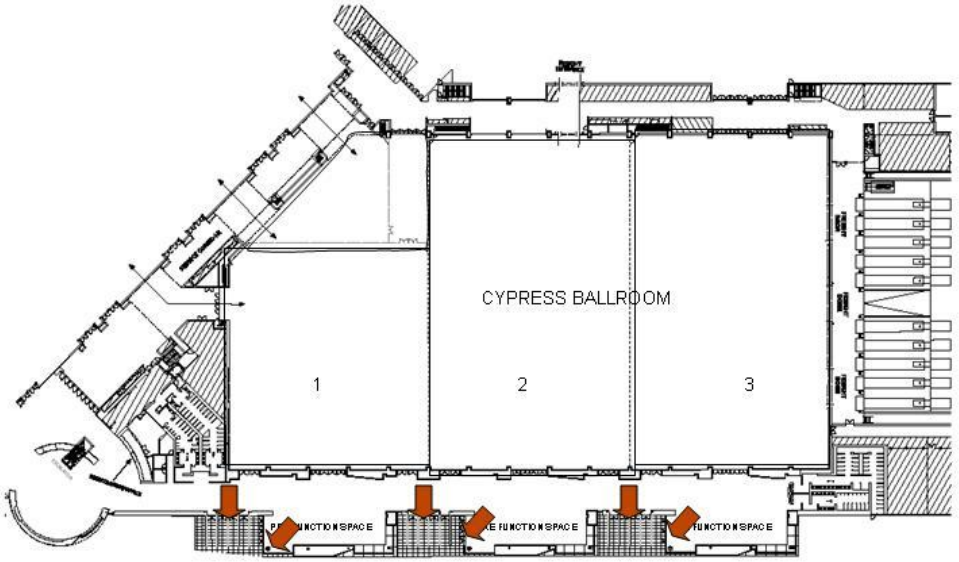
- Speaker name: Tyler Williams
- Speaker title: Co-Founder and Vice President of Business Development
- Company name: Wurldtech
- Location: The Hague, Netherlands

Your safety is important to us
Please be aware of these emergency procedures

- In the event of an emergency please dial ext. 55555 from any house phone. Do not dial 9-1-1.
- In the event of an alarm, please proceed carefully to the nearest exit. Emergency exits are clearly marked throughout the hotel and convention center.
- Use the stairwells to evacuate the building and do not attempt to use the elevators.
- Hotel associates will be located throughout the public space to assist in directing guests toward the closest exit.
- Any guest requiring assistance during an evacuation should dial “0” from any house phone and notify the operator of their location.
- Do not re-enter the building until advised by hotel personnel or an “all clear” announcement is made.

Your safety is important to us
Convention Center exits in case of an emergency





Know your surroundings:

- Identify the meeting room your workshop is being held in
- Locate the nearest exit

The Achilles™ Practices Certification Program

The Industrial Cyber Security Landscape

The Past: *Security What?*

The Achilles™ Practices Certification Program

The Industrial Cyber Security Landscape

The Present: *I Got It, I Got it, No, I Got It*

The Achilles™ Practices Certification Program

The Industrial Cyber Security Landscape

The Future: *Poor Sisyphus*

The Achilles™ Practices Certification Program

The Industrial Cyber Security Landscape

The Zeitgeist

You're Under Attack?

The Technology

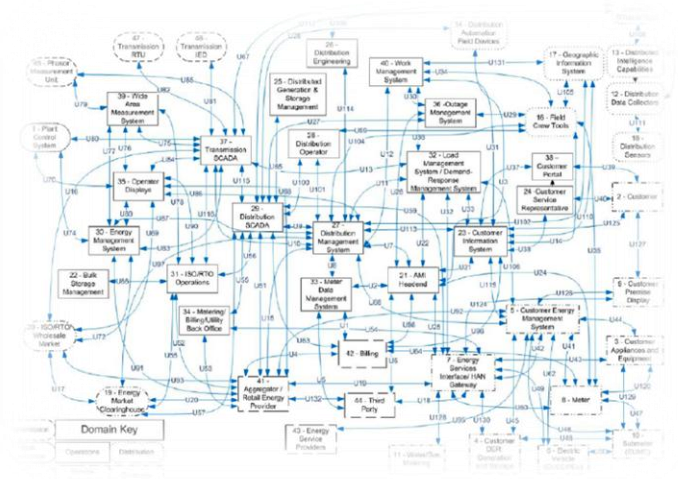
What Do You Expect?

The Achilles™ Practices Certification Program

The Industrial Cyber Security Landscape

The Direction

Too Far Too Fast



The Communication

Can You Hear Me Now?

The Achilles™ Practices Certification Program

The Industrial Cyber Security Landscape

The Stakeholders

We're Secure!

The Business Environment

Stuxnet, Stuxnet….Stuxnet

The Achilles™ Practices Certification Program

The Industrial Cyber Security Landscape

The Standards Efforts

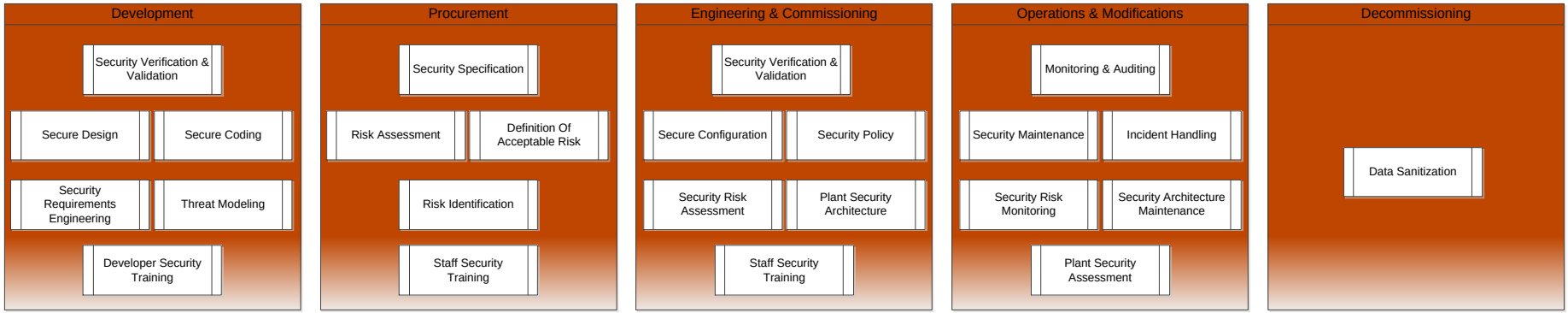
"Workinggroupitis"

The Results

It Looks Right…Kind Of

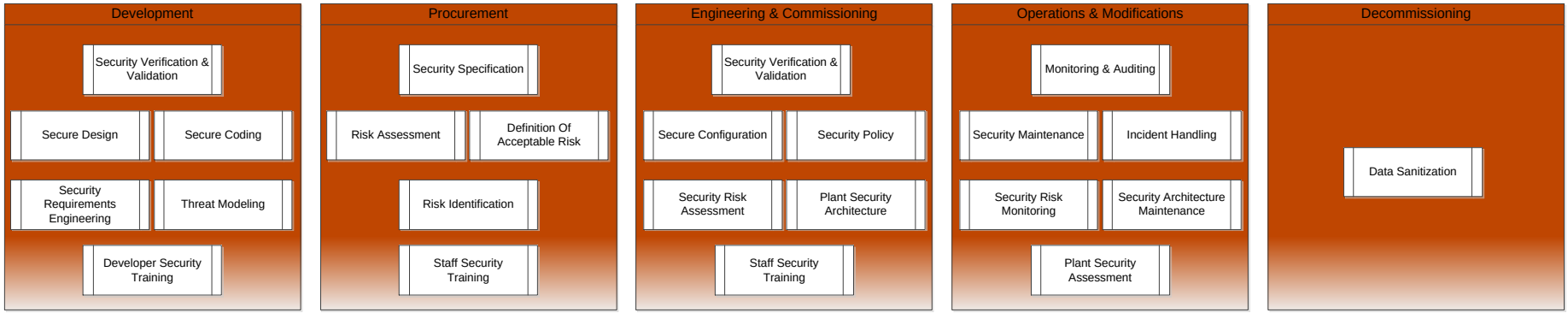
How to get the security you need
A walk through the life cycle of an industrial control system

Security in industrial control systems...
... a process – not a product



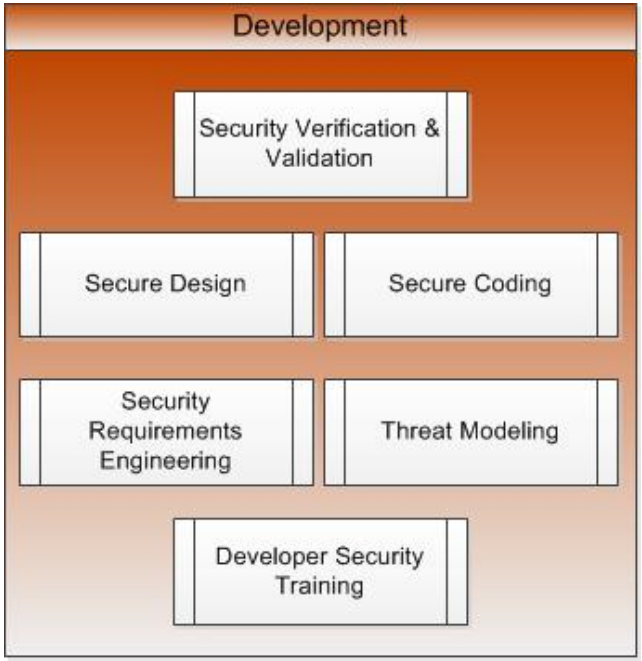
- "Security is a process, not a product" (B. Schneier)
  - Several processes are required to obtain security
  - Processes must cover the entire system lifecycle
- Security is a "moving target"
  - Technology advances over time (offensive and defensive)
  - Attack schemes and attackers change over time
  - System operation changes over time

Security in industrial control systems...
... is a shared responsibility



- System lifecycle must cover
  - Product development
  - System procurement
  - System engineering and deployment
  - System operations and modifications
- Between different phases the primary responsibility shifts
  - Vendors
  - System integrators
  - Asset owners & operators

Security process in software product development
Achieving generic product security



Main responsible:

- Product vendor

Organizational preparation

- Security training & awareness

Product security specifications

- Security requirements engineering
- Threat modeling
- Tool support available

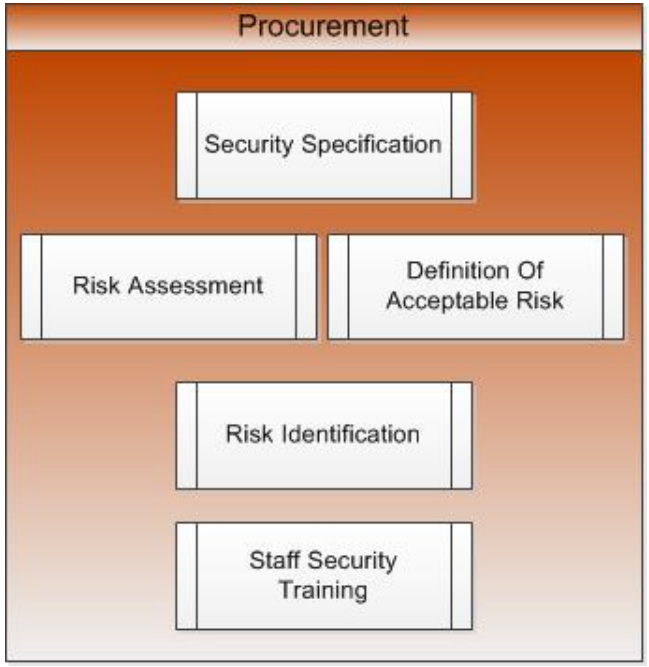
Secure implementation

- Secure design patterns
- Secure coding standards
- Tool support available

Security verification and validation

- Robustness testing
- Security test cases
- Some tool support available

Security process in control system procurement
Sepcifying site-specific system security



Main accountable:

- Asset owner

Organizational preparation

- Security training & awareness

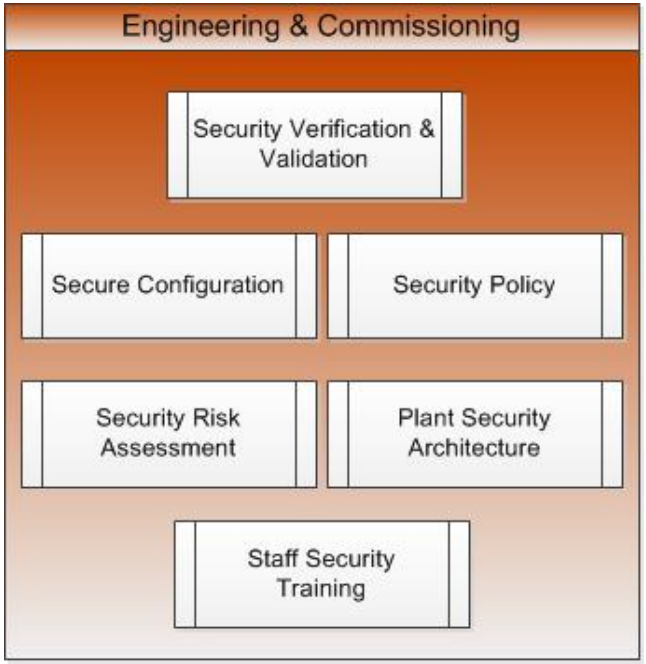
Risk management

- Risk identification
- Risk assessment
- Definition of acceptable risk

System specification

- System security requirements to mitigate the identified, untolerable risks

Security processes in engineering and commissioning
Achieving site-specific system security



Main responsible:

- Asset owner/operator

Support from:

- Product vendor
- System integrator

Organizational preparation

- Security training & awareness

Establish security context

- Plant-specific security risk assessment
- Plant-specific security architecture

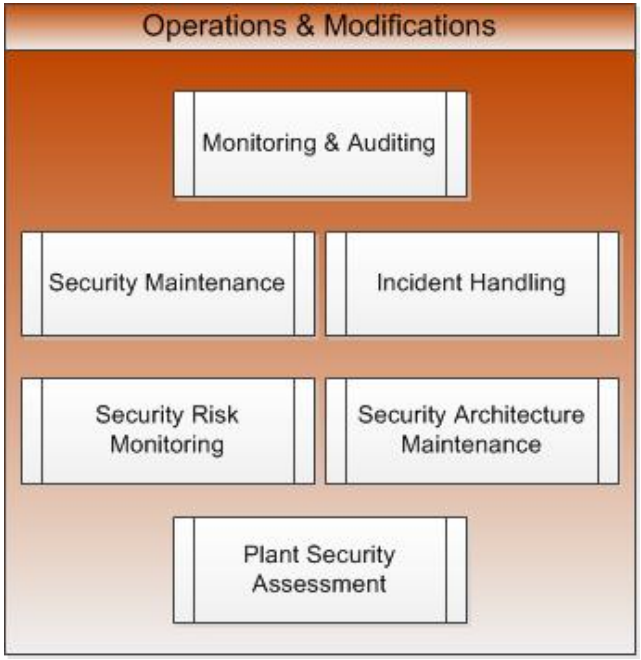
Security setup

- Organization-specific security policy
- System-specific security configuration

Security verification and validation

- Security test cases in FAT/SAT
- Security sign-off

Security processes in operations and modifications
Maintaining site specific system security



Main responsible:

- Asset owner/operator

Support from:

- Product vendor
- System integrator

Periodic checks

- Plant security assessment

Security context

- Security risk monitoring
- Security architecture maintenance

Maintaining site security

- Security policy management
- System maintenance, e.g.
  - Patch management
  - Account management

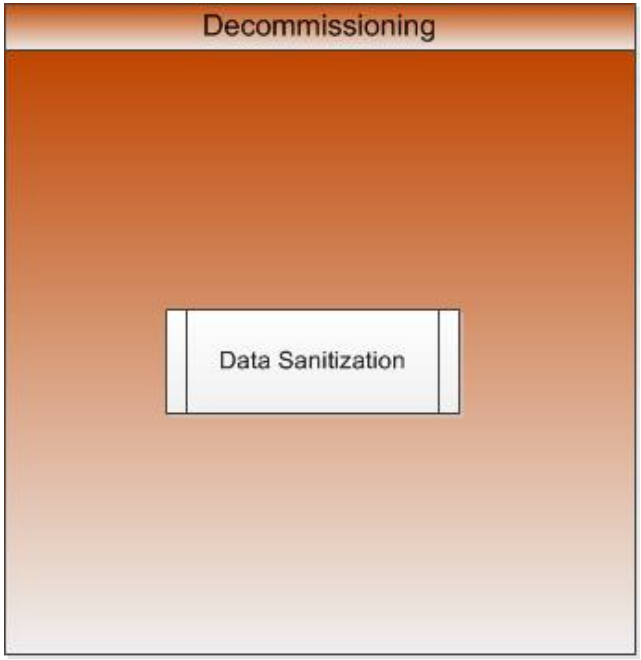
Incident handling

- Disaster management
- Communication with external parties

Continuous situational awareness

- Monitor & audit logs

Security process in control system decommissioning
Maintaining site-specific security beyond operations



Data sanitization

- Identify sensitive data
- Remove sensitive data

Main responsible:

- Asset owner

Conclusion

Security is a process

- Continuous efforts are needed
- Must span the entire lifecycle
- Must adapt to the changing environment

Security is a shared responsibility

- Vendors, system integrators and asset owners/operators each have their responsibility and need to work together

Reminders
Automation & Power World 2011

- Please be sure to complete the workshop evaluation
- Professional Development Hours (PDHs) and Continuing Education Credits (CEUs):
  - You will receive a link via e-mail to print certificates for all the workshops you have attended during Automation & Power World 2011.
  - BE SURE YOU HAVE YOUR BADGE SCANNED for each workshop you attend. If you do not have your badge scanned you will not be able to obtain PDHs or CEUs.

Power and productivity
for a better world™