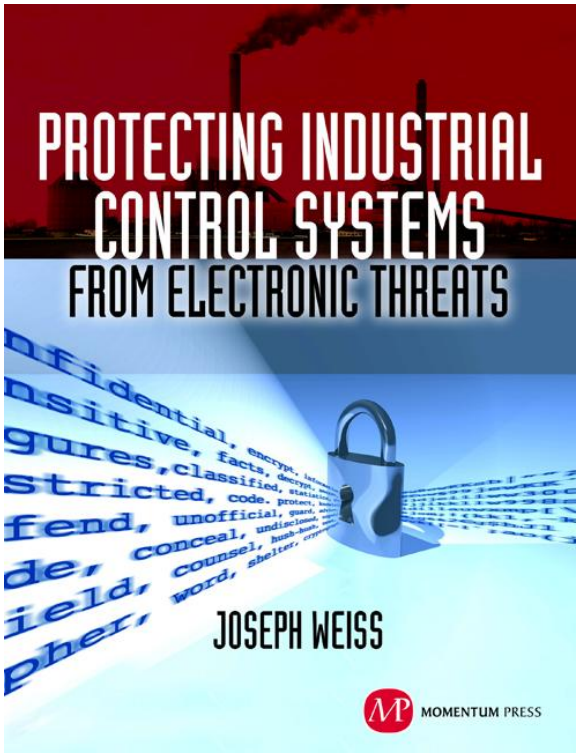
Industrial Control System (ICS) Cyber Security

NAWC

October 7, 2013

Joe Weiss
PE, CISM, CRISC, ISA Fellow
(408) 253-7934
joe.weiss@realtimeacs.com



Control Systems Basics

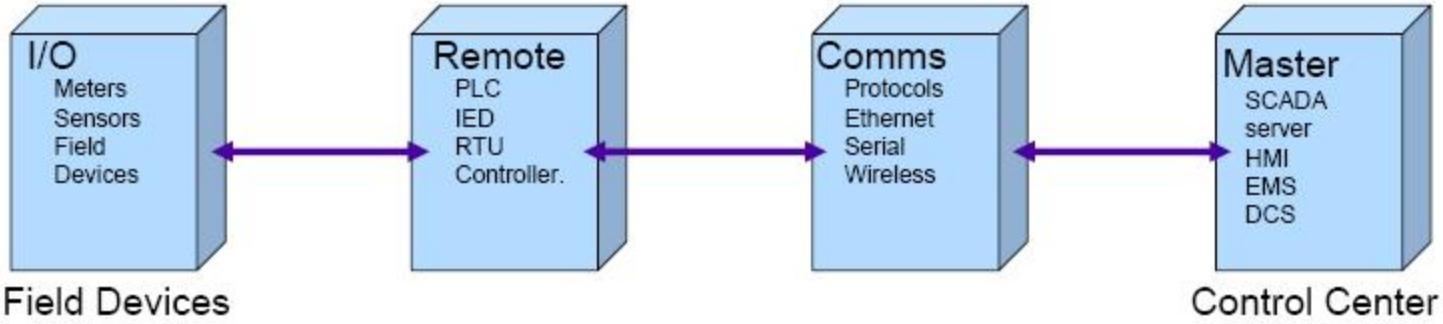
Sensors

Motor Controls

Control Valves

Programmable Logic Controllers (PLC)

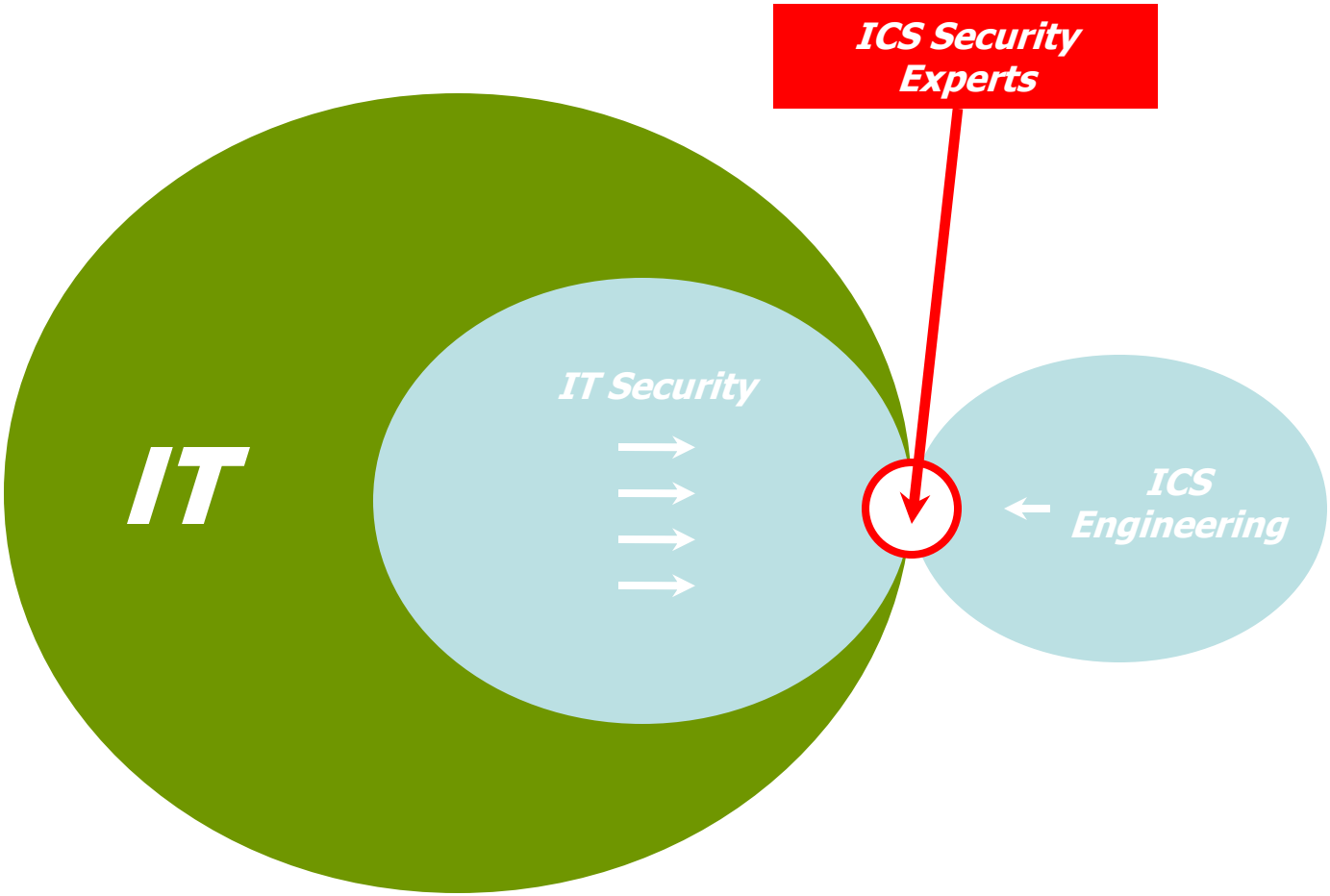
Human Machine Interfaces (HMI) and Operator Displays



Important Considerations

- Modern ICSs with remote connectivity provide many productivity benefits but come with ICS cyber vulnerabilities
- ICSs are different than IT
  - ICS cyber forensics and logging is minimal at best
    - There will probably be a cyber Pearl Harbor but you won't know it is cyber because of the lack of ICS cyber forensics
  - ICS cyber threats are not just the network but insecure engineering designs/features that cannot be patched (see Stuxnet and Aurora)
    - A good attacker wanting to cause damage will go after the engineering features
  - Securing ICSs is a trade-off between performance and security
    - Performance must win but by how much
  - It takes ICS experts that understand the domain and IT experts that understand security working together to secure ICSs

ICS Security Expertise Lacking



ICS Cyber Incidents and Water

- There have already been >25 actual control system water/waster cyber incidents
  - Many were intentional
- Project Shine identified >1,000,000 directly Internet facing control system devices
- ICS Honeypot - why should you care
  - Control systems were Internet facing with no security
  - Small rural water utility attracted hacks from all over the world
  - Many attempted to control water system
  - Minimal ICS cyber forensics
  - …

What Needs to be Done

- Have Senior Management buy-in
- Develop ICS cyber security policies, procedures, and awareness
- Include security as part of the design basis
- Recognize potential reliability and safety issues with digital systems
- Treat security as an engineering issue
- Know what you have installed
- Develop relevant ICS cyber forensics and training
- Include IT, operations, equipment vendors, plant designer, and incident responders as a team
- Work with utility test bed