



MeOH Flo









Me O H Flo

#### Senior Systems Engineer Engineering Control Ltd 10+ years experience Control Systems (DCS/PLC) Safety Systems (TÜV FSE 7040/13) Industrial Networks (Ethernet/fibre) Server Management (Windows) Current role PCD IT Cyber Security (contract) with STOS **IDC Safety Control Systems &** Hazardous Areas Conference Auckland, 22-23 August 2017

**Presenter – Peter Jackson** 



#### Why is ICS Security Important?

IEERING CONTROL

- Control/SCADA systems control "real-world" devices and processes
- Cyber attacks on a control/SCADA system can lead to serious consequences
- Cyber "security level" generally needs to provide more risk reduction than required safety integrity level for SIF to be effective.



#### Process Industry Standards Related to Cyber Security



MeOH Flo

- IEC 61508 Functional Safety of Safety-Related Systems
- IEC 61511 Safety Instrumented Systems for the Process Industry
- ISA / IEC 62443 Cyber Security Suite of Standards
- ISA TR84.00.09 Cyber Security related to Function Safety process



#### The Time for Cyber Security is Now

Standards for cyber security
Cyber security breaches impact
Networked facilities
Cyber attacker capabilities
Potential to shutdown process, change display, impact productivity







### The threat is real

Specifically targets Siemens PLCs

- Introduced by USB flash drive
- May have destroyed up to 1000 centrifuges

#### German steel mill attack

Stuxnet

- "...manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in 'massive' damage"
- Hacked into Office Network
- ... then production management software
- ... then plant control systems





#### The threat is real

KT02010\_CAE\_AODT

ECL\_CAE\_AODT \_\_\_

Black Energy malware

 In December 2015, around half the homes in the Ivano-Frankivsk region in Ukraine were left with no electricity for a few hours. According to reports, the cause of the 6-hour power outage was a cyber-attack that utilized malware. Interestingly, the reported case was not an isolated incident, as other electric firms in Ukraine were found to have also been targeted.

Deployment via email





#### - - - C In1 - - - C In2 C In3 C In4

#### But we have a firewall

Is the firmware up to date? What about zero-day vulnerabilities? Are the logs reviewed? Has it been configured to a design? Design documentation maintained? Least privilege? Are the 'holes' so large that a hacker could drive straight through?







### **Other Cyber Security Myths**



- - Air gapping is enough Security by obscurity is a protection Only Windows PCs are at risk (lvl2) ICS cybersecurity threat is overblown It won't happen here because it
    - hasn't happened before



### **Six questions - Crowe Howarth**

(TD2010\_CAE\_AODT)

ECL\_M2\_AODT\_

1. Cybersecurity program in place?

- 2. Designated cybersecurity leader?
- 3. Cybersecurity team understands the role?
- 4. Procedures specifically for detecting and containing cyberattacks?
- 5. Plan for responding to cybersecurity incidents?
- 6. Does our plan include testing, assessments and continuous improvement?





### **Cyber Security Best Practice**

Policies and Procedures **Network Segregation** ▣. Physical Access Control **System Hardening User Access Control** Malicious Software **Prevention/Whitelisting** Antivirus Patching **Backups** Logs **Performance Monitoring & Alerting** 



#### FAQ – What do I do with old stuff

# These security concepts are great Unrealistic to retrofit entire plant

- Solutions available for legacy devices:
  - Become knowledgeable about ICS security and industry standards
  - Protect legacy devices and systems with security device
  - Can be installed in live systems without harm to production
  - Allows rules to be tested and changed without putting plant operations at risk





#### Defence in Depth – Bank Analogy

#### T02010\_CAE\_AODT

#### )n Req

## Purdue model (levels 0 to 4) Bank has multiple layers of protection

- Security guards course access control
- Security-trained tellers fine access control
- Steel doors simple barriers (open/closed)
- Bullet proof windows
- Security box keys allows access to specific authorised entities

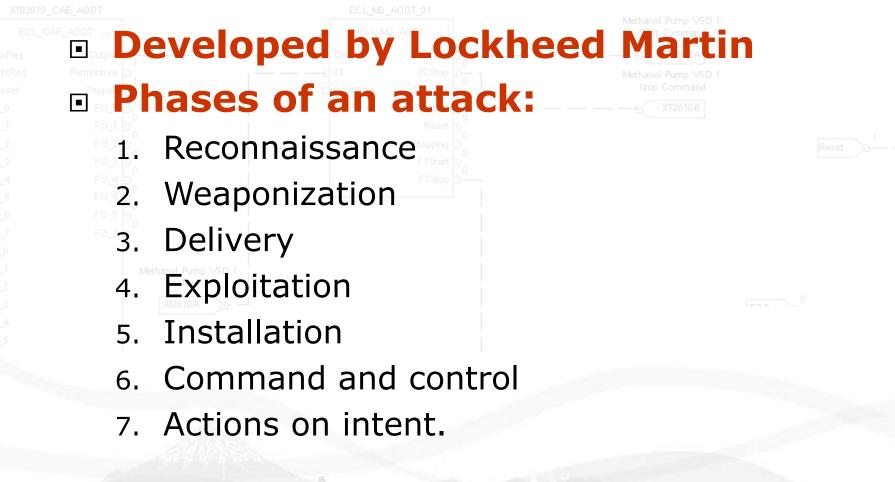
#### Layers are context specific

- Each layer provides some protection
- Overall protection provided by layers working together





### Cyber Kill Chain®









### IT and OT

MeOH Flo

 Information Technology
 Level 4+
 Servers/PCs

- People focus
- Lifetime 3-5 years
- Server focus
- Confidentiality and integrity focus

Operational Technology

- Level 3-
- All configurable devices
- Device focus
- Lifetime 15-20 yrs
- End-point focus
- Safety and availability focus





### **Practical Cyber Security Steps**





- 7. Involve Management
- 8. Detect & Response Plan



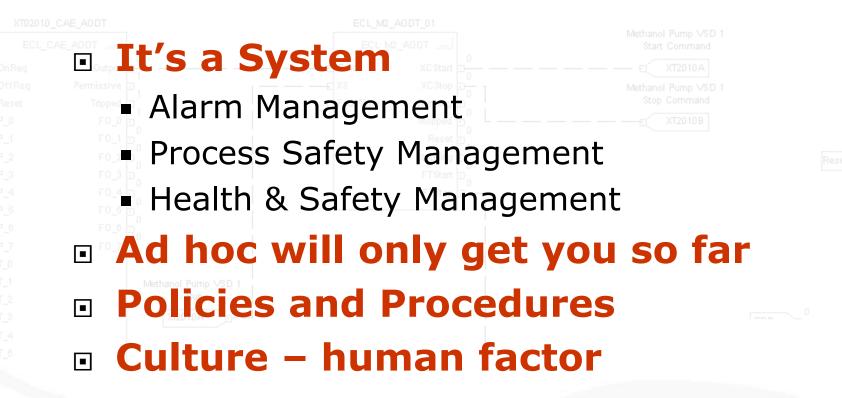


#### e In2 E In3 E In4

MeOH Flo

SL020

### **Cyber Security 101**





**ECL Offering** 



MeOH Flo

# Report – audit, identify, advise Project manage – mitigations, actions Training – empower your control system engineers

- Implement put new barriers in place, strengthen existing barriers
- Maintain cyber security is a process not an event

