KASPERSKY lab

Industrial Cybersecurity 2018:
Opportunities and challenges in Digital Transformation

MARTY EDWARDS

International Society of Automation (ISA)
USA

- Globally recognized ICS cybersecurity expert with 25-year experience
- Director of Strategic Initiatives for the ISA
- Managing Director of the Automation Federation
- Was the longest-serving Director of the U.S. DHS ICS-CERT

@ICS_Marty

Setting the Standard for Automation™

THINK LIKE A HACKER … but ACT LIKE AN ENGINEER!

Marty Edwards
Director of Strategic Initiatives – ISA
@ICS_Marty

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Definitions…

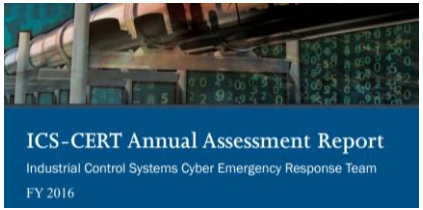
I use the term “Hacker” to talk about the good guys – White Hats.

Unfortunately – the media thinks all hackers are evil. Criminals, Black Hats – and all of them wear hoodies

Control System History Lesson

Information Technology	Operational Technology
Lean towards computer science	Lean towards engineering
Cybersecurity savvy	Safety savvy
New computer every 3 years	New ICS every 30 years
Patch the system every day	Expect the vendor to patch for them
Loss of a single client computer is a reasonably low impact event	Loss of a single controller can be a catastrophic event
Mostly concerned about Confidentiality of data (breaches)	Mostly concerned about Integrity of data and Availability of systems
Everything on the Internet 	Everything on the Internet 

Everything is connected to everything!

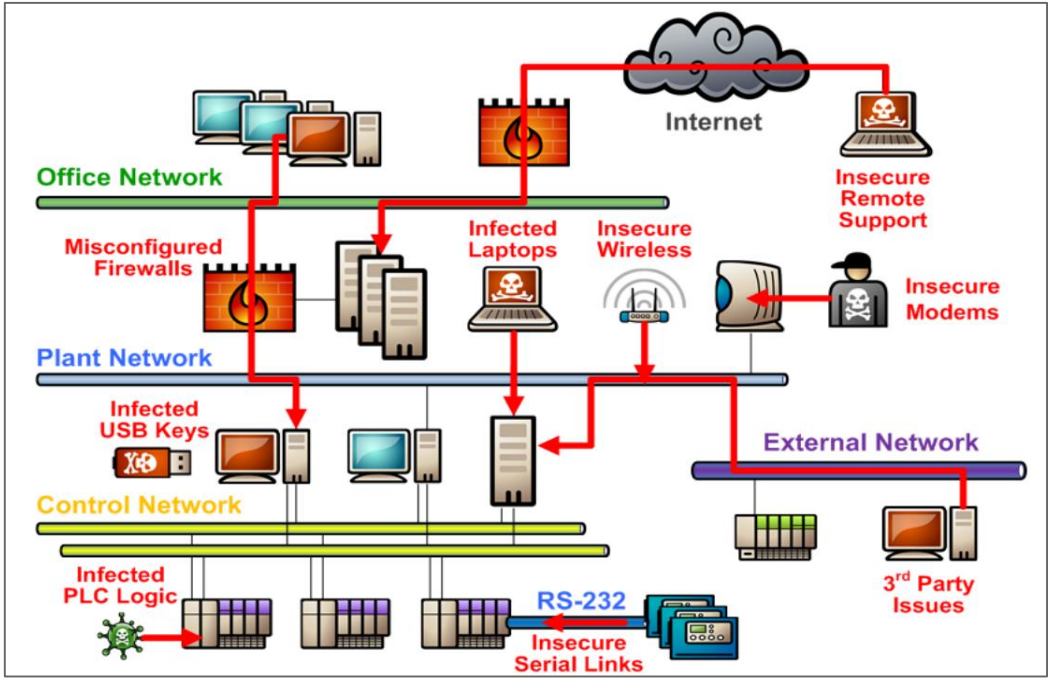


FY 2014-2017 Top Six Weakness Categories in Order of Prevalence			
FY 2014	**FY 2015**	**FY 2016**	**FY 2017**
1. Boundary Protection	1. Boundary Protection	1. Boundary Protection	1. Boundary Protection
2. Access Control Policy and Procedures	2. Least Functionality	2. Least Functionality	2. Identification and Authentication (Organizational Users)
3. Least Privilege	3. Authenticator Management	3. Identification and Authentication (Organizational Users)	3. Allocation of Resources
4. Remote Access	4. Identification and Authentication (Organizational Users)	4. Physical Access Control	4. Physical Access Control
5. Physical Access Control	5. Allocation of Resources	5. Audit Review, Analysis, and Reporting	5. Account Management
6. Information System Monitoring	6. Least Privilege	6. Authenticator Management	6. Least Functionality

Table 1: FY2014-FY2017 Top Six Weaknesses.

System segmentation is still a huge issue!

Most OT has multiple entry points



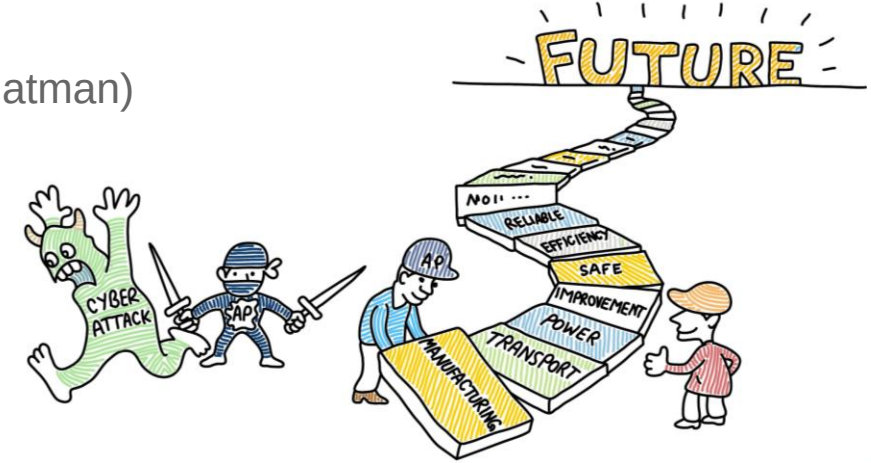
Tofino Security / Eric Byres – Using ISA/IEC 62443 Standards to Improve Control Systems Security – May 2014

- Insecure Remote Access
- Firewall and Network Misconfiguration
- Infected Laptops
- Insecure Modems
- Infected USB drive
- Insecure Wireless
- And so on…

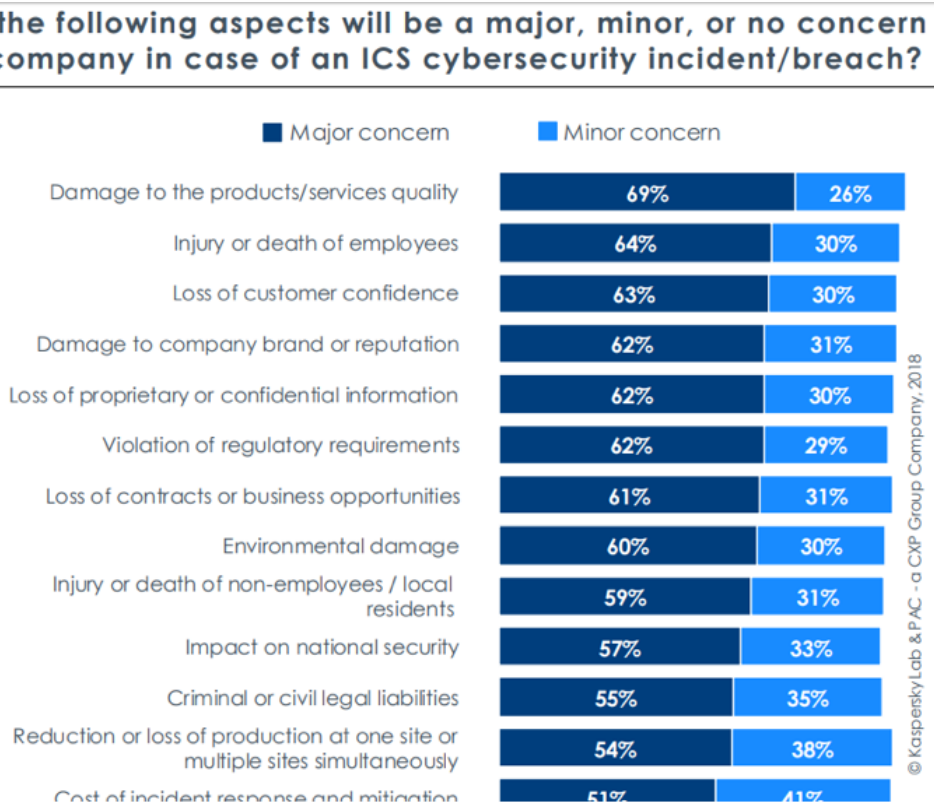
Lots of bugs and malware can affect ICS/OT

- Commodity OS Malware (MS08-067 / Conficker)
- Common Library Vulnerabilities (SSL / Heartbleed)
- Ransomware Infections (CryptoLocker / Petya)
- Intelligence Collection (HAVEX / BlackEnergy)
- IT Destructive / disk wiper (Shamoon)
- OT Destructive / firmware bricking (BlackEnergy 3)
- Surgically Targeted (Stuxnet)
- Physical Destruction (Triton / Trisis / Hatman)

- What will the future bring ???



What are we concerned about?



Survey Says –

Top two categories are of Major Concern:

“Damage to the product”

“Injury or Death”

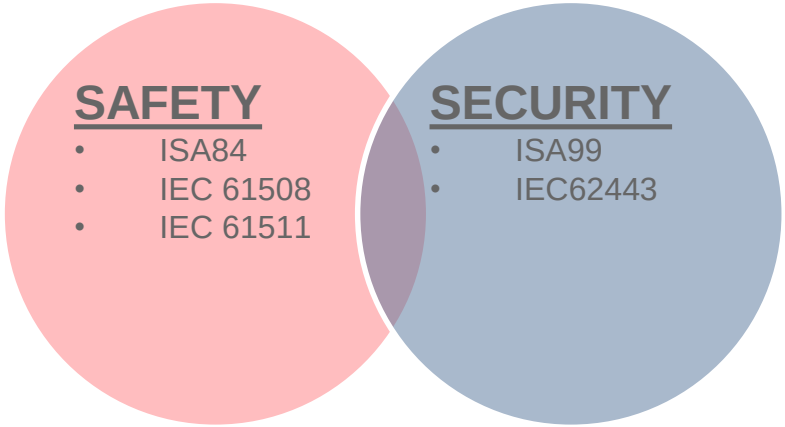
Houston we have a problem (actually two…)

1) We have critical safety systems that are now network accessible and often integrated closely with the “Basic Process Control System” (BCPS) and enterprise / business systems

2) We have been trying to patch and update every system without considering which ones are the most important – “no risk assessment”

If everything is important then nothing is.

It is time to consider BOTH Safety and Security as one in ICS/OT design



Stop ignoring the fundamentals

- **PROBLEM:**
  - Cyber attacks on Industrial Control Systems (ICS) and/or Operational Technology (OT) can have significant physical consequences
- **SOLUTION:**
  - Apply sound engineering principles, and consider cyber induced consequences when designing and building systems

Acknowledgement / Disclaimer – This presentation is based upon a series of works entitled “Consequence-Driven, Cyber-Informed Engineering (CCE)” developed by the Idaho National Laboratory (INL). The presenter has collaborated with the INL on this presentation and has obtained their permission to utilize this material.

This requires several different skills

Adversary

CONSEQUENCE PRIORITIZATION

- How can I cause the most significant damage to your process?

Analyst

SYSTEM OF SYSTEMS BREAKDOWN

- Is there a cyber-based control system involved?
- Where are the dependencies?

H4XØR

CONSEQUENCE BASED TARGETING

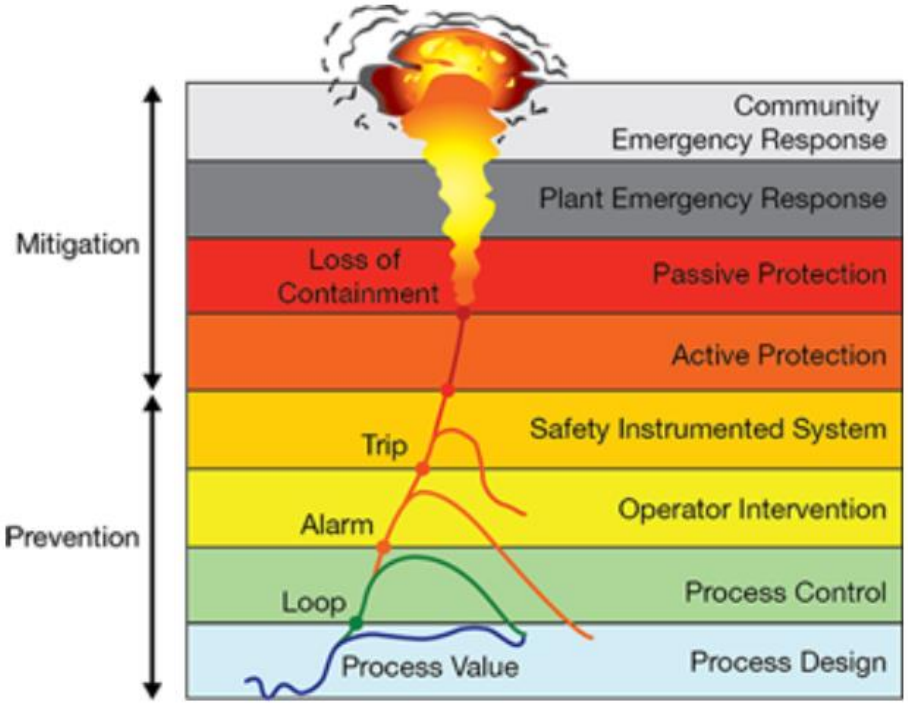
- Where can I attack the system using cyber means?
- Map the ICS Kill Chain

Engineer

MITIGATION & PROTECTION STRATEGIES

- Design out the cyber risk
- This is NOT application of control system cybersecurity!

Focus on the most significant consequence



- Find that one part of your process that if everything failed would be considered a significant disaster
- Remember these?
  - Bhopal India (1984)
  - Flixborough England (1974)
  - Texas City (2005)

First you need to know what systems exist

- Asset discovery / inventory – this can be hard in the OT space
- First step of the NIST Framework

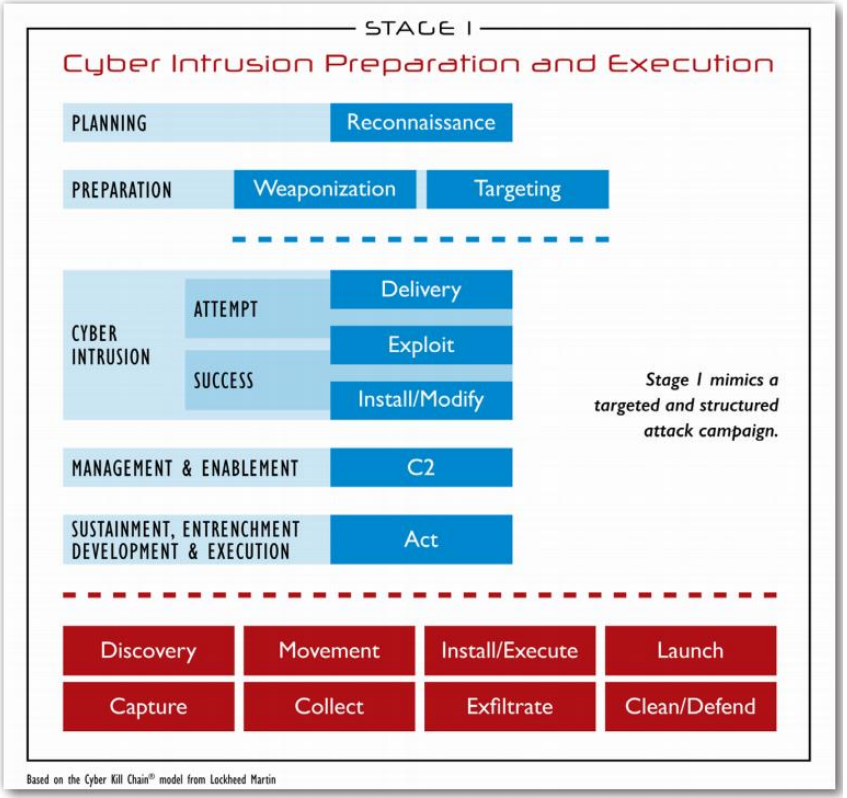
IDENTIFY

“Know your enemy and know yourself …”

Sun Tzu – The Art of War

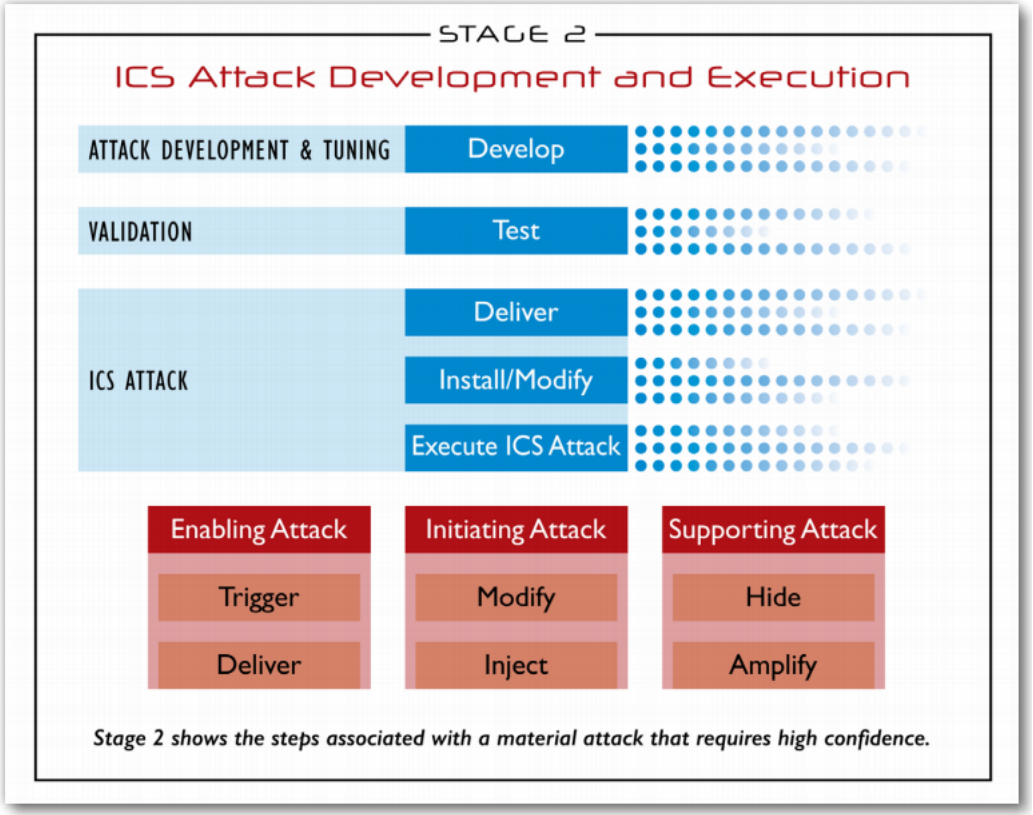
Credit: N. Hanacek/NIST

Next – Evaluate pathways into those systems



- This is where the attacker gains an initial foothold
- Various methods:
  - SpearPhishing
  - Waterhole
  - Insider
- Can be targeted or not (opportunistic)
- Each step has an effective defense to disrupt the attack
- Attacker will attempt to maintain persistent access
- Most of the time the malware is not ICS specific

Stage 2 – Execute attack on the target ICS



- Once access is obtained, then the attacker can carry out their plan
- Intelligence Gathering / Exfiltration
- IP Theft
- Data modification or destruction

- Now the malware will have to be ICS or system specific

Step 4 – Non-cyber mitigations / protections

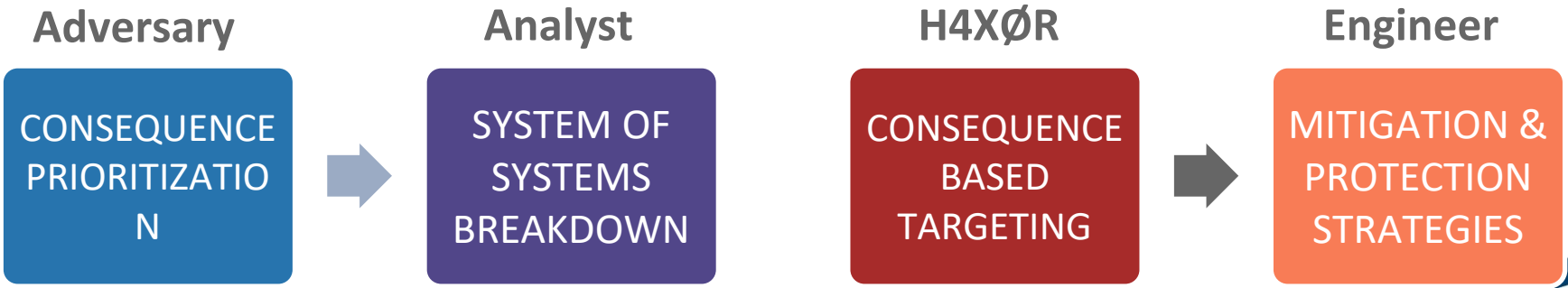
GOAL

- Develop an engineering based control to eliminate the cyber risk to critical functions -- completely
  - Hardwired interlock
  - Mechanical protection
  - Custom analog and digital circuitry
- No this isn't going "backwards" – this is prudent use of technology
- Not applicable to every process

Think like a hacker but act like an engineer!

- Identify your most critical business or operations function
- Understand what systems, controls or devices support it
- Determine how an attacker would cause the most damage by compromising the cyber integrity of any of that equipment

- Go back to basics – find a way to accomplish the function without relying on a cyber device. After all, it is your most important function!
- Build a culture of security and safety around cyber-physical systems

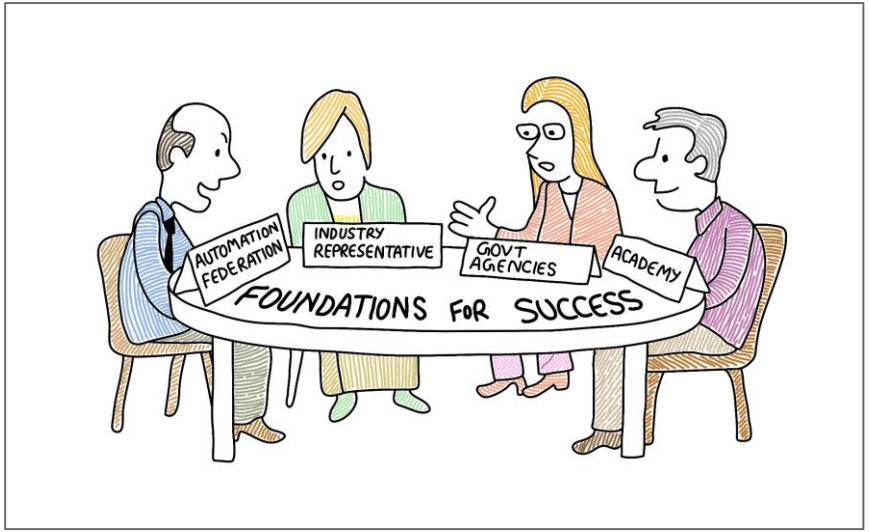


For more information

@ICS_Marty

Join ISA Today !

- Local sections all over the world
- Free access to ISA's Globally Recognized, Consensus Based Standards
  - ISA99 / IEC62443 (Cybersecurity)
  - ISA84 / IEC61508 / 61511 (Safety)
  - And many many others!
- Discounts on training, publications
- Visit us at: www.isa.org



Setting the Standard for Automation™