RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SBX4-W4

Safety Systems are the New Target Design Security Using Safety Methods

Marty Edwards

Director of Strategic Initiatives
International Society of Automation (ISA)

@ICS_Marty

Disclaimer …

- In this presentation I use examples from several commercial companies. The presenter has collaborated with these companies and has obtained permission to use their material. Mention of these company names or their products is not an endorsement of them by myself or ISA.
- Some material in this presentation is based upon a series of works entitled “Consequence-Driven, Cyber-Informed Engineering (CCE)” developed by Idaho National Laboratory (INL). The presenter has collaborated with the INL and has obtained their permission to utilize this material.

December 2017 - TRITON / TRISIS Hits the news

FireEye

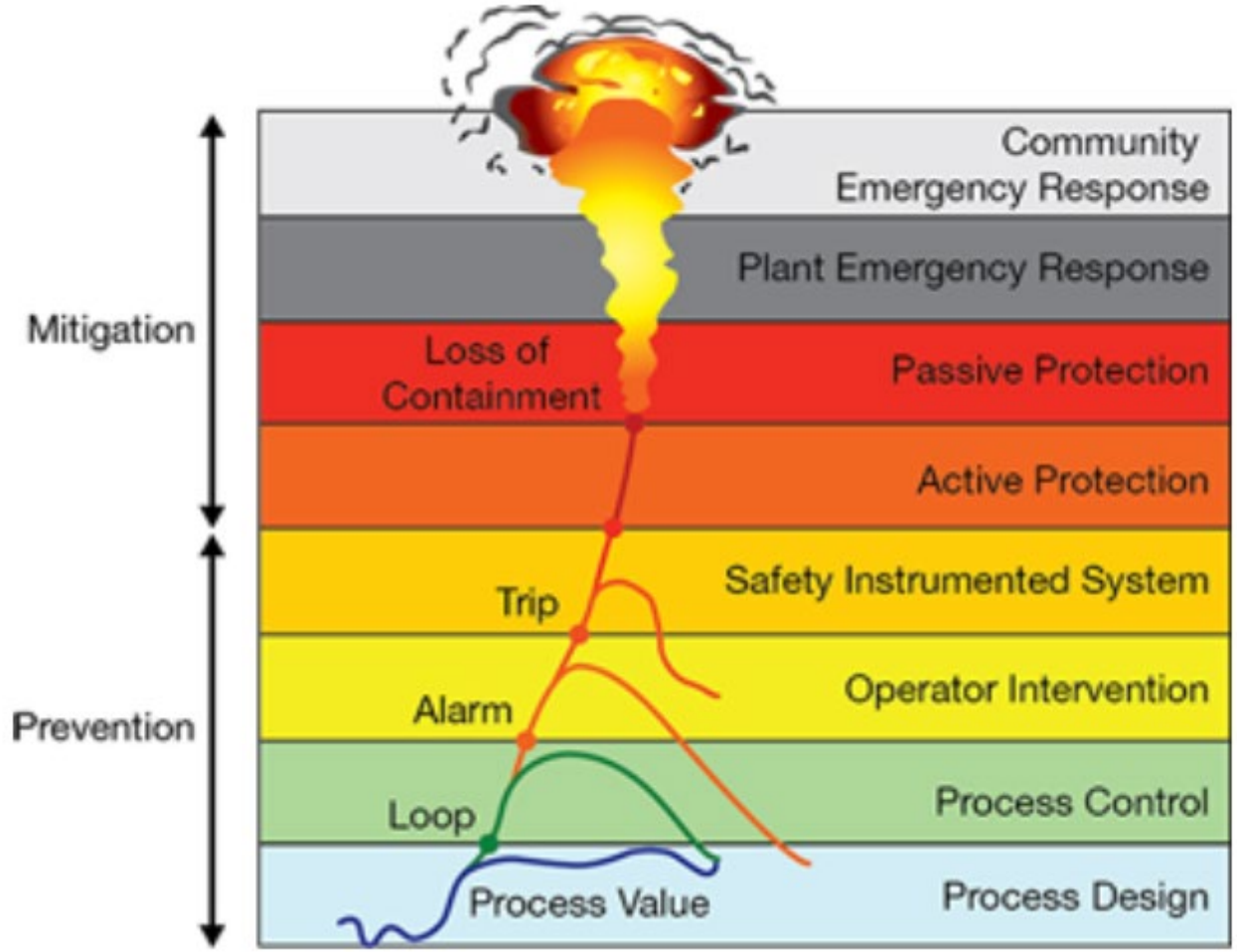
Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure

December 14, 2017 | by Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer

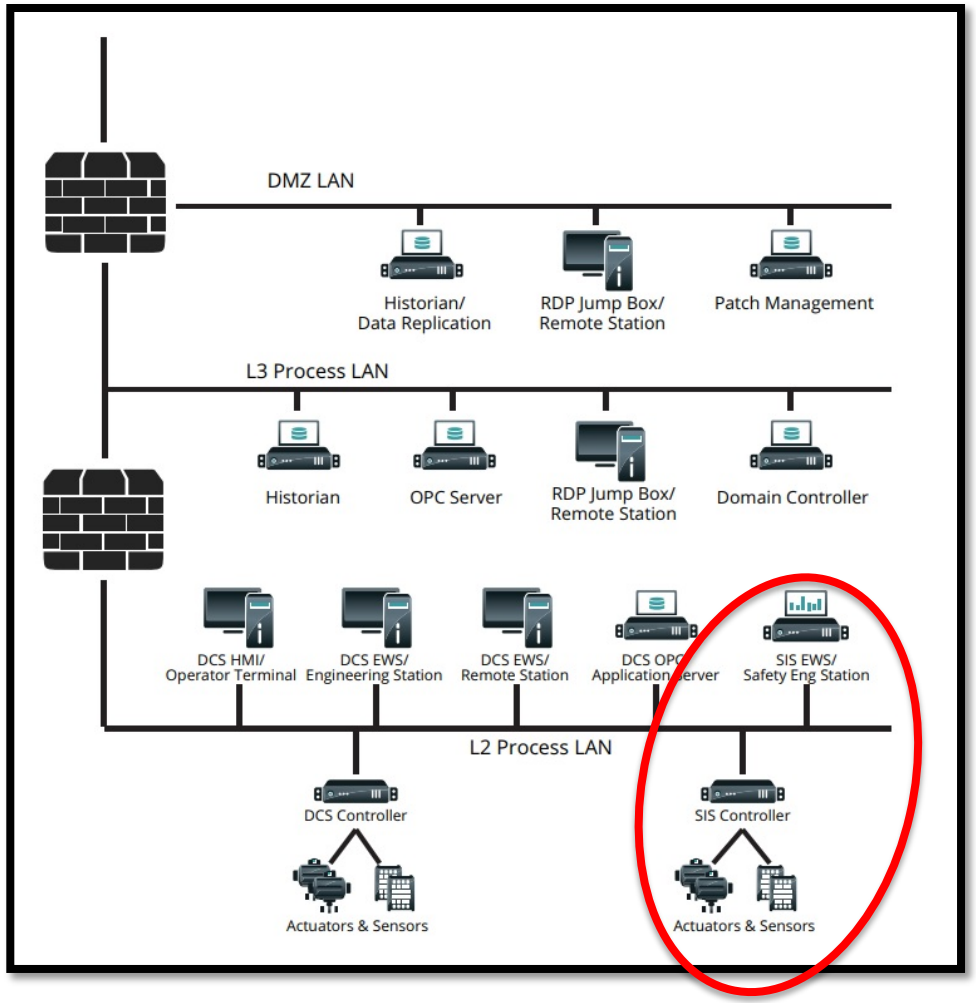
- Attackers targeted the "Safety Instrumented System" or SIS of a Critical Infrastructure organization in the Middle East

Review - SIS Overview

- The SIS is the “last line of protection”
- Typically a very fault tolerant industrial computing device(s) that monitor sensor conditions and shut down a process that is becoming dangerous
- Very specialized, and designed using rigorous functional safety methodology and standards



Review - Insecure SIS Implementation



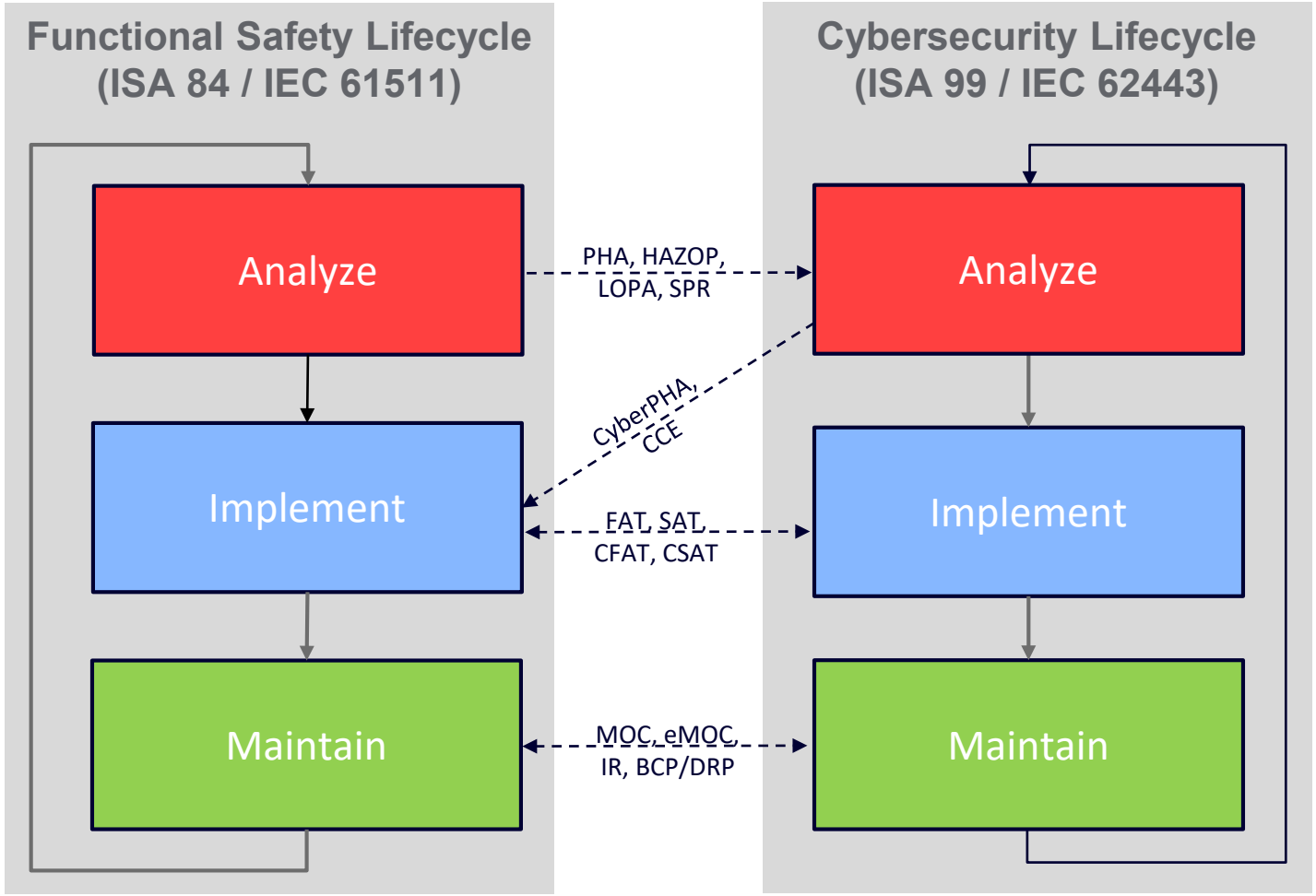
- SIS should NOT be accessible from any other network
- Use isolation techniques, unidirectional gateways, etc.
- Attackers gained access to the Engineering Workstation and then modified the programming in the SIS controllers
- Resulting in an unplanned shutdown event (fail safe)

Question to ask – “Why?”

- Why did the system designers make this mistake ??
- Are there engineering processes or procedures to make sure we don’t make the same mistake in the future ??
- The good news is “YES” !!
- We can apply “Functional Safety Analysis” to Cybersecurity

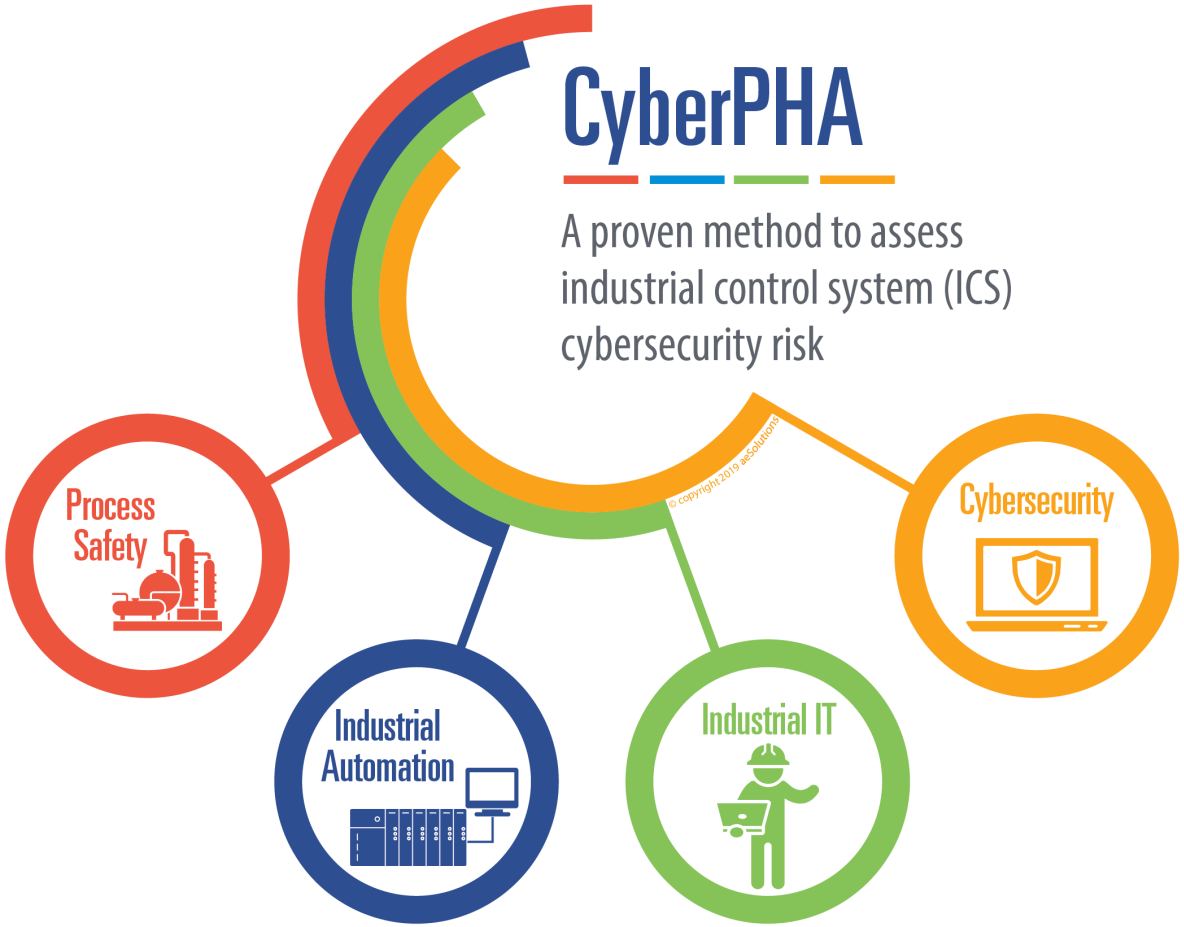
Illustration by Chris Gash

Integrating Functional Safety with Cybersecurity



- Traditionally, different disciplines
- Yet process safety is dependent upon both
- Integration is critical
- Leverage maturity of safety risk analysis
- Integration at “Analyze” phase is key

Cyber Process Hazard Analysis (PHA)

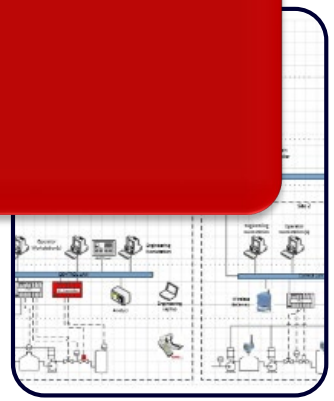


Cyber PHA

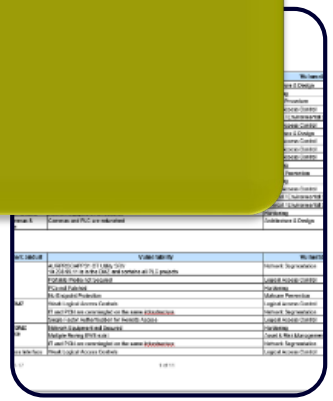
A safety-oriented methodology to conduct a security risk assessment for an ICS / SIS

Multi-step, Rigorous Methodology

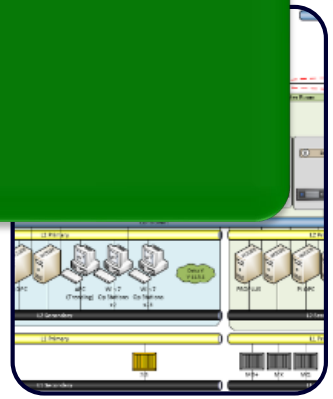
Document System
- Arch Diagram
- Inventory
- Dataflows



Vulnerability Assessment
- Networks
- Endpoints
- Physical
- Policies / Procedures

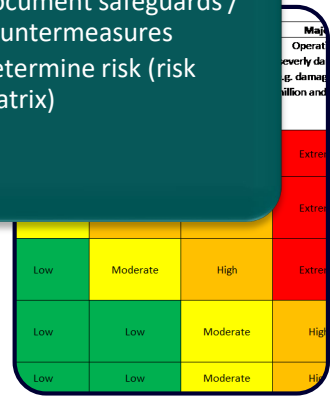


Partition System
- Zones & Conduits
- Catalog vulnerabilities by zone



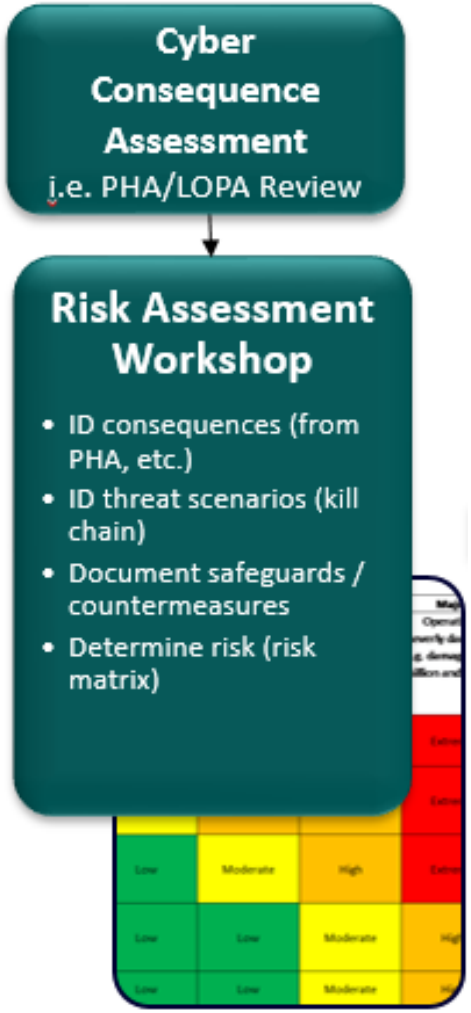
Cyber Consequence Assessment
i.e. PHA/LOPA Review

Risk Assessment Workshop
- ID consequences (from PHA, etc.)
- ID threat scenarios (kill chain)
- Document safeguards / countermeasures
- Determine risk (risk matrix)



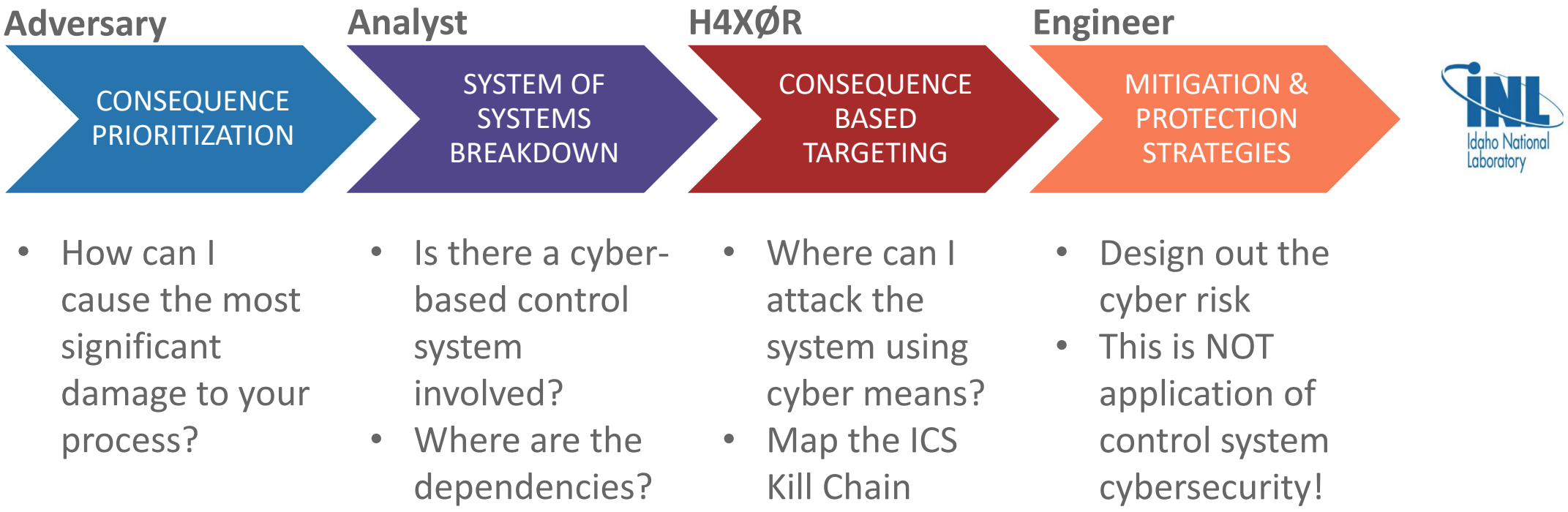
Mitigation Planning
- Develop mitigations (technical, procedural or mechanical)
- Risk Ranked and Prioritized

Risk Assessment Workshop – Consequence Driven



- <u>This is the crucial step !!</u>
- Identify the consequences of failure (including cyber induced) using established methods
  - Process Hazard Analysis (PHA)
  - Layer Of Protection Analysis (LOPA)
- Identify threat scenarios
- Document safeguards and countermeasures
- Develop a Risk Register

Consequence-Driven Cyber-Informed Engineering (CCE)



- Multiple step process, requiring a diverse team of experts with different skills. Ask the hard questions – and solve the hard problems

Security PHA Review (SPR)
"Hackable" Safeguards – Yes or No ?

KENEXIS
DESIGNED FOR SAFETY, SECURITY & RELIABILITY

Kenexis Open PHA - /Volumes/james.mcglone@kenexis/Shared/Kenexis Data/Training Courses/Security PHA Review/Exercise Solutions.opha

Study Data | Nodes | Deviations | PHA Worksheets | LOPA Worksheets | Recommendations | Safeguards | Parking Lot | Risk Criteria | Premium Tools

PHA Worksheets

4. Exercise #4 - Tank Reactor Runaway Reaction

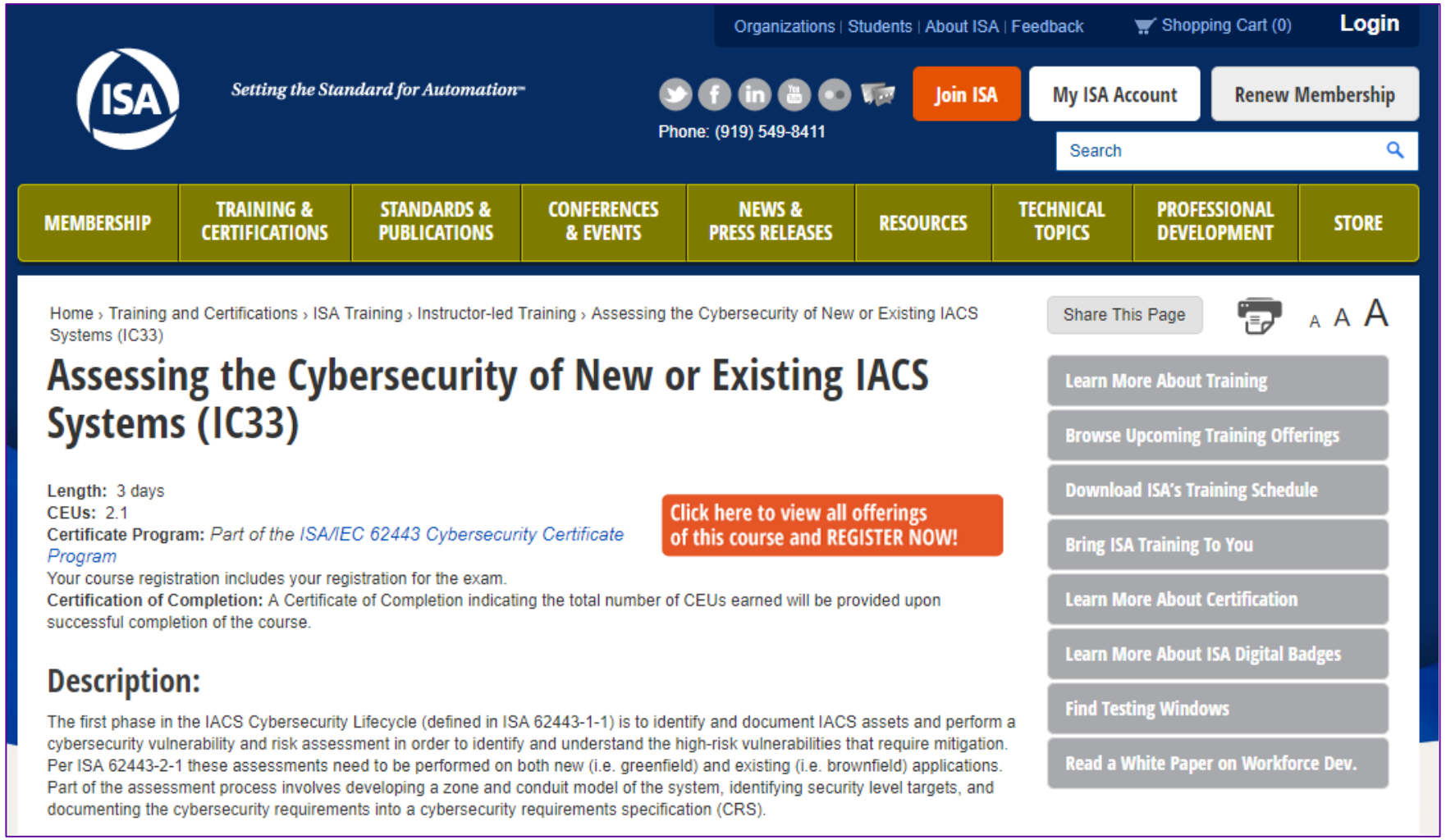
Search Worksheet...

Deviation	Causes: Cause	Causes: Cause Hackable	Consequences: Consequence	S	L	RR	Safeguards: Safeguard	Safeguards: Safeguard Hackable	Scenario Hackable	PHA Recommendation
4.1 High Pressure	4.1.1 Failure of Cooling Water Pump P-403, which results in loss of cooling water flow to Cooling Jacket E-402 of Reactor R-401	Yes	4.1.1.1 Once the flow of cooling water is stopped, the heat of reaction begins to build up in teh reactor, resulting in high temperatures. A runaway reaction will the start resulting in thermal decomposition of product C into gaseous byproducts and a rapid increase in pressure in the reactor beyond the maximum allowable working pressure. Loss of containment of process material with physical explosion. Potential fire and potential vapor cloud explosion. Potential single fatality is expected to operator or maintenance in area of reactor.	H	M	3	8 Safety Instrumented Function UZC-403 dumping the reactor contents into the quench vessel which stops the reaction.	Yes	Yes	8 Consider implementing an analog SIF mimic in parallel with the existing safety instrumented function. 9 If inherently safe against cyber-attack safeguards are not implemented, consider Implementing cyber security countermeasures at SL 2 for this zone.

Apply What You Have Just Learned

- Ask your plant engineers – do we have anything covered by:
  - Process Safety Management (PSM)
  - Environmental Protection Agency (EPA) Risk Management Plan (RMP)
  - Department of Homeland Security (DHS)
    Chemical Facility Anti Terrorism Standards (CFATS)
- Do we conduct any of the following:
  - Hazard And Operability Study (HAZOP)
  - Process Hazard Analysis (PHA)
  - Layer of Protection Analysis (LOPA)
- If the answer is yes – then you should investigate adding consequence-driven cyber-informed engineering to them

ISA Has Training Available!



Q&A – 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

- Dragos Report
  - https://dragos.com/wp-content/uploads/TRISIS-01.pdf
- FireEye Blog / Report
  - https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
- Idaho National Laboratory CCE
  - https://www.osti.gov/biblio/1341416-consequence-driven-cyber-informed-engineering-cce
- International Society of Automation (ISA) Standards
  - https://www.isa.org/standards-publications/