

RSA®Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

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



#RSAC

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.

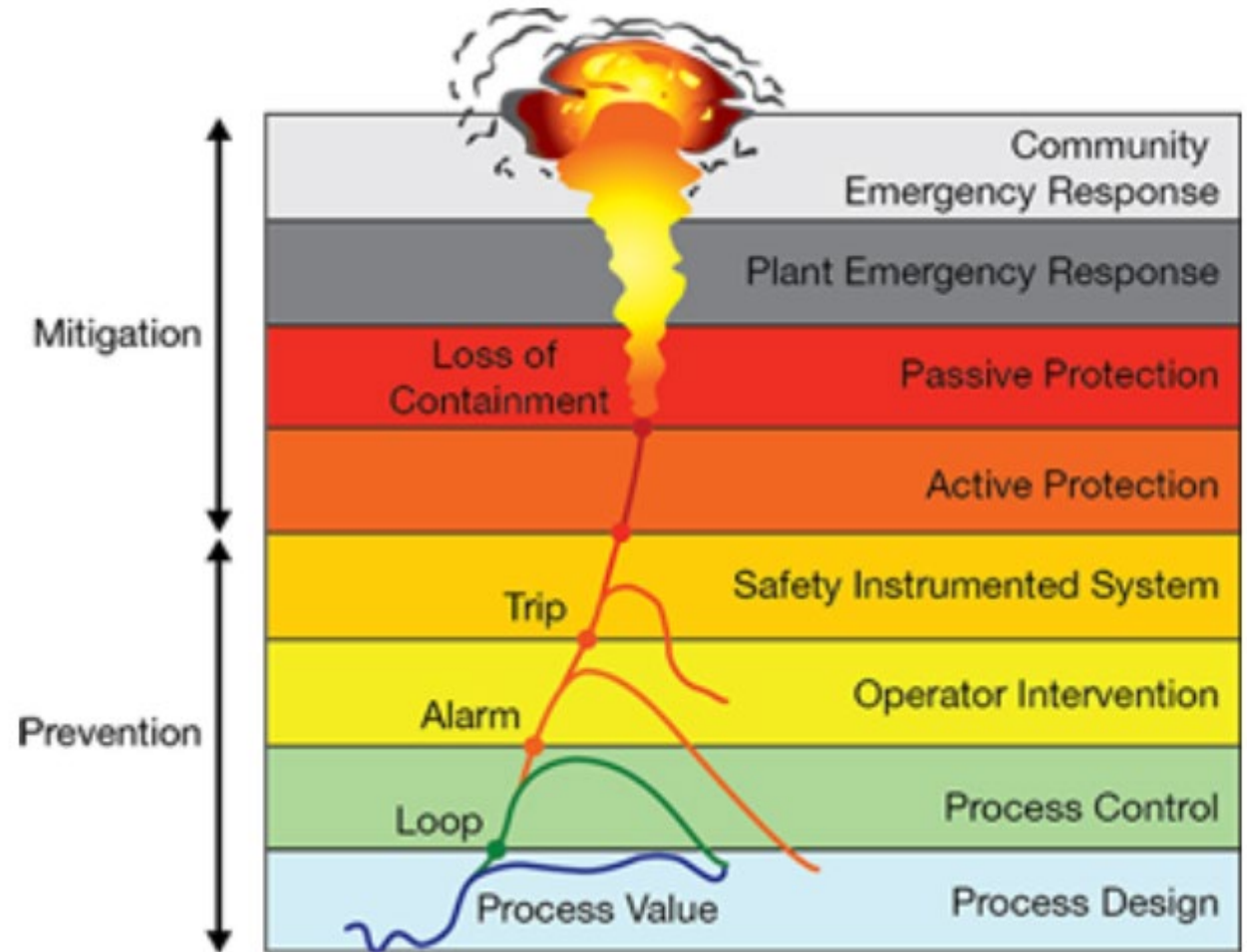
December 2017 - TRITON / TRISIS Hits the news



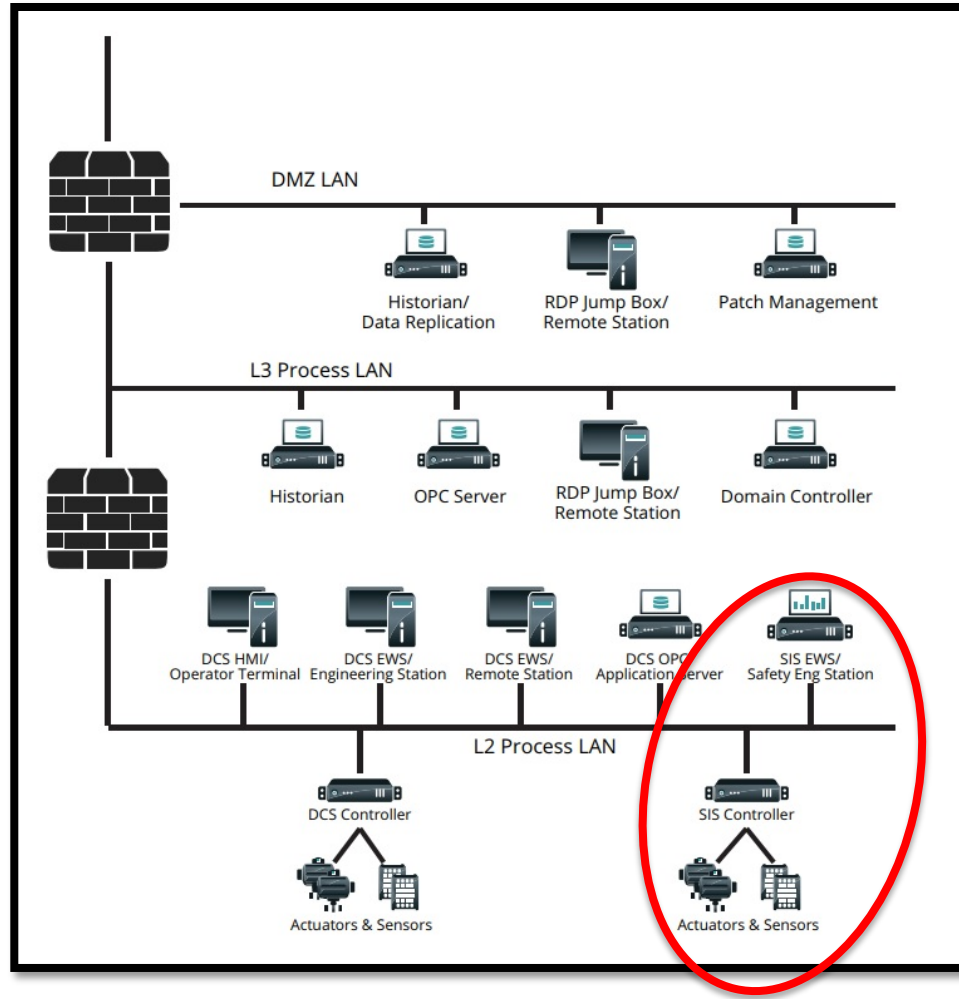
- Attackers targeted the “Safety Instrumented System” or SIS of a Critical Infrastructure organization in the Middle East

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)

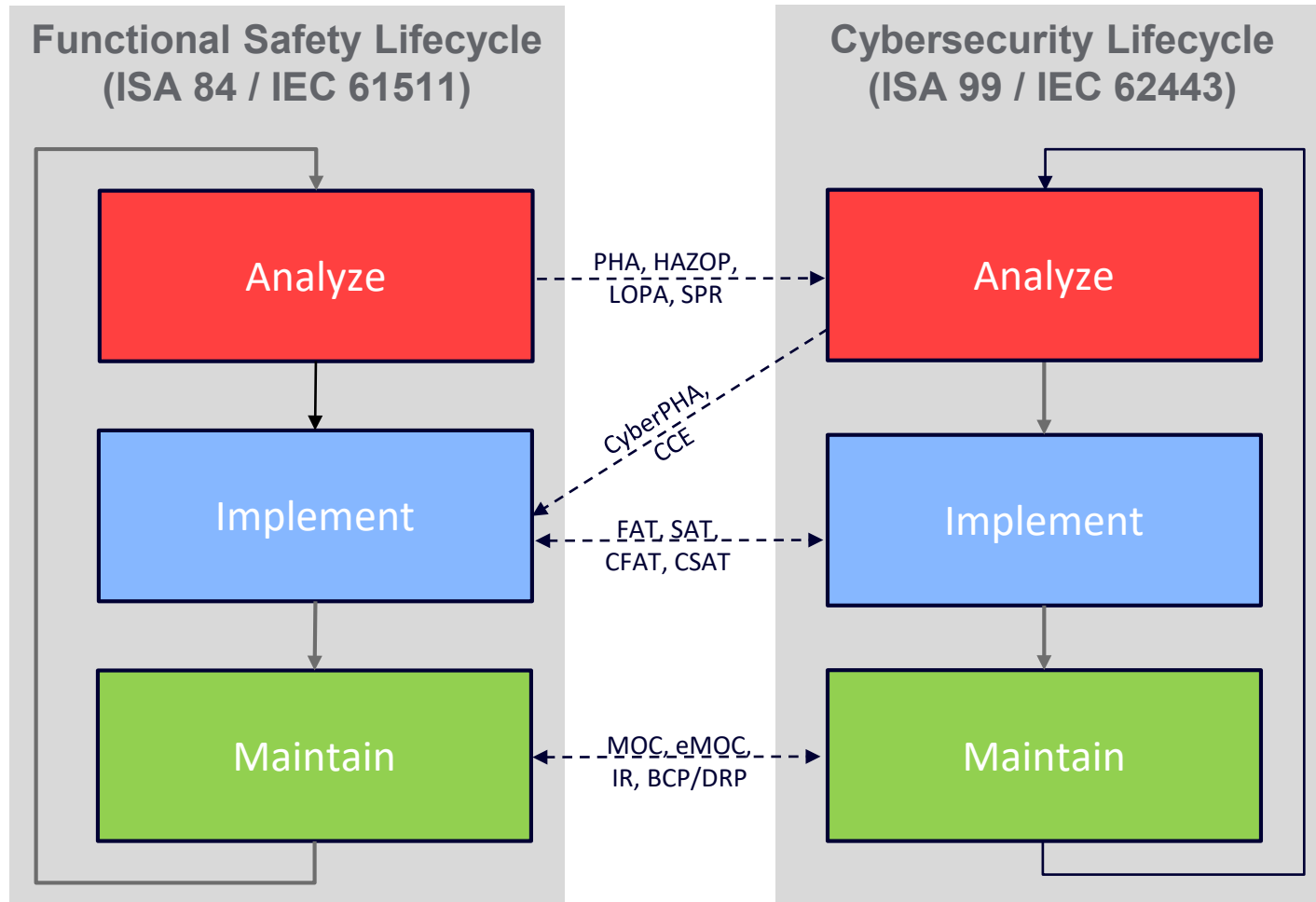
Question to ask – “Why?”

- 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



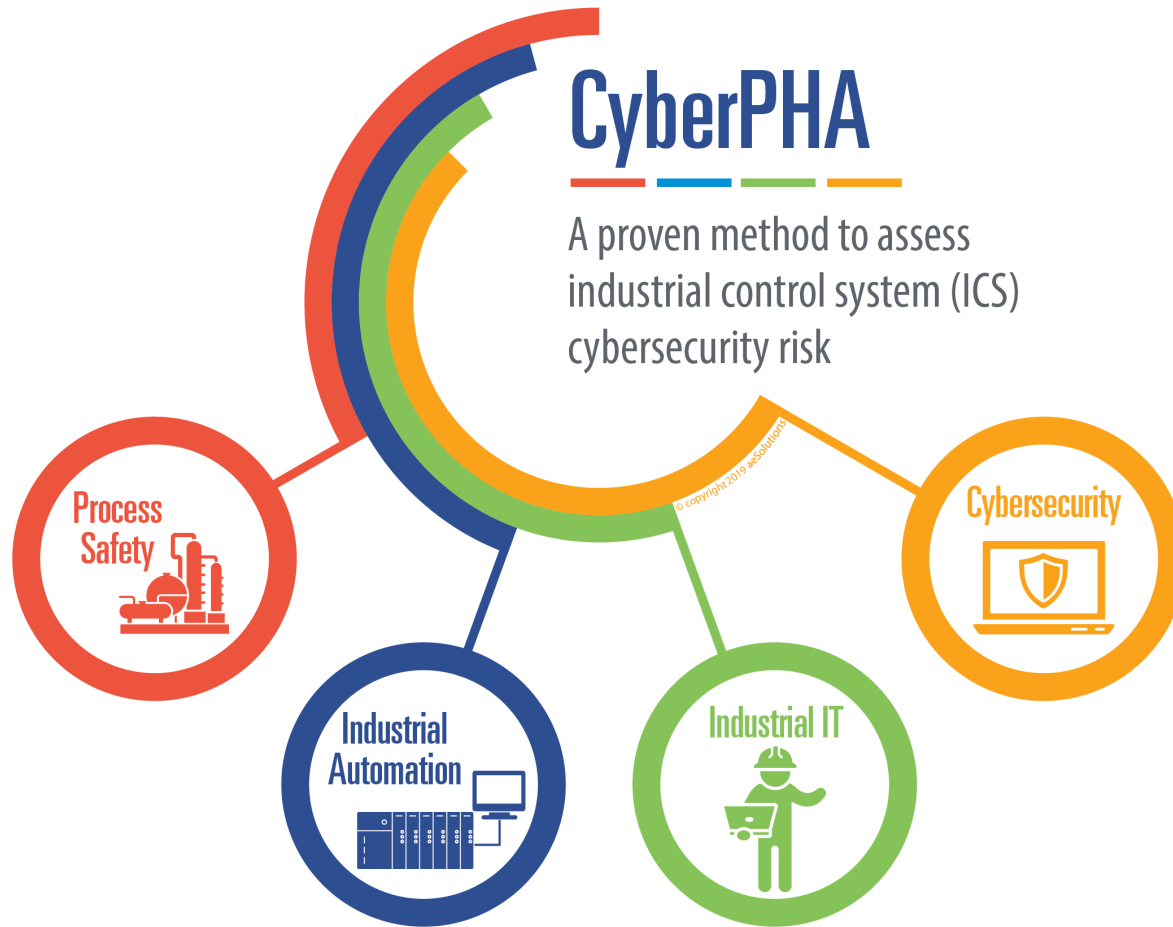
Illustration by Chris Gash

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

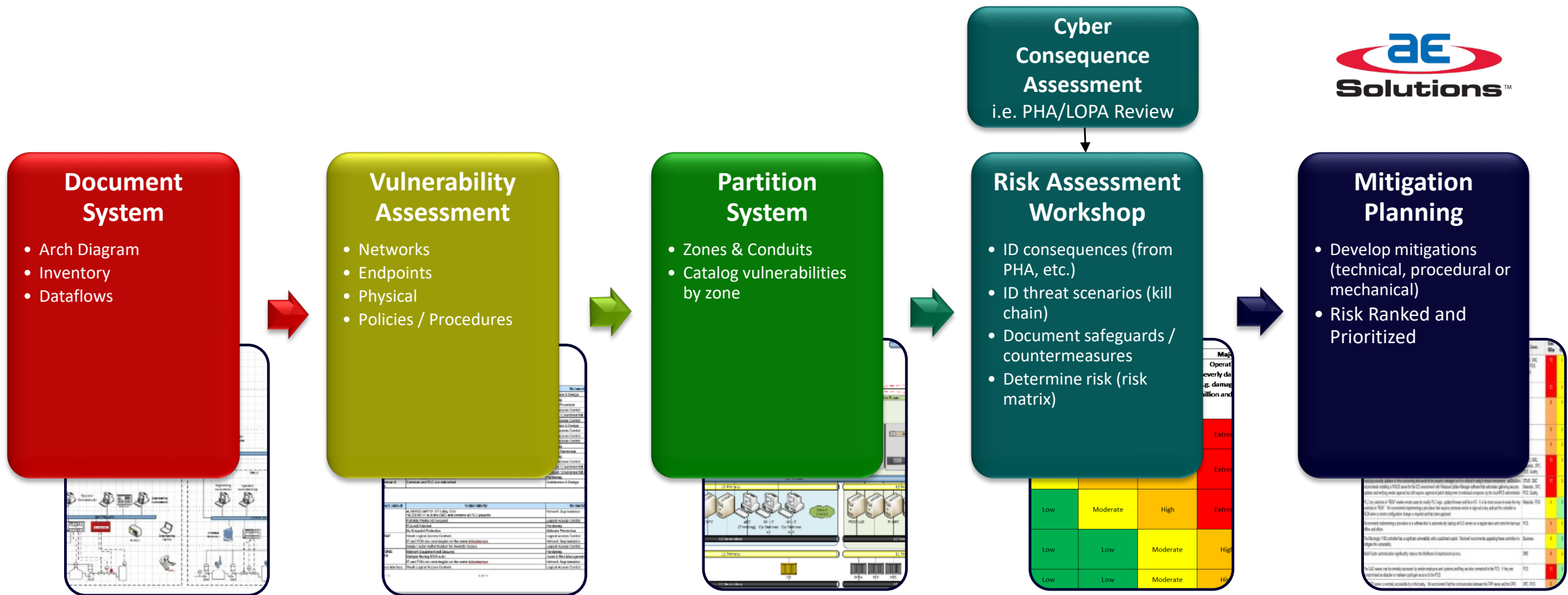
Cyber Process Hazard Analysis (PHA)



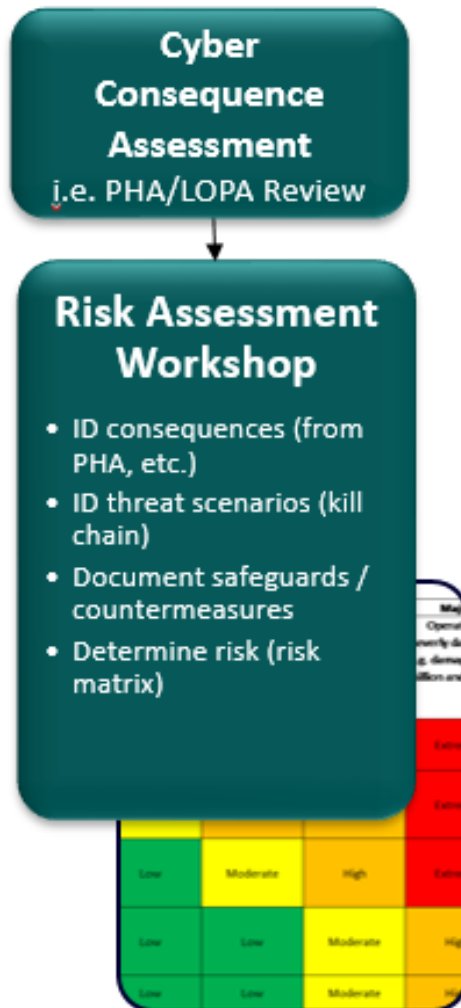
Cyber PHA

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

Multi-step, Rigorous Methodology



Risk Assessment Workshop – Consequence Driven



- This is the crucial step !!
- 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)



- How can I cause the most significant damage to your process?
- Is there a cyber-based control system involved?
- Where are the dependencies?
- Where can I attack the system using cyber means?
- Map the ICS Kill Chain
- Design out the cyber risk
- This is NOT application of control system cybersecurity!

- 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 ?



Study Data

Nodes

Deviations

PHA Worksheets

LOPA Worksheets

Recommendations

Safeguards

Parking Lot

Risk Criteria

Premium Tools

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

PHA Worksheets

4. Exercise #4 - Tank Reactor Runaway Reaction

+

📄

✂

📄

🗑

⬆

⬆

||

🔍

🔍

||

📄

⬆

⬇

↔

Search Worksheet...

Deviation	Cause	Cause Hackable	Causes								PHA Recommendation
			Consequence	S	L	RR	Consequences		Scenario Hackable		
							Safeguards				
							Safeguard	Safeguard Hackable			
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	<div>8 Consider implementing an analog SIF mimic in parallel with the existing safety instrumented function.</div> <div>9 If inherently safe against cyber-attack safeguards are not implemented, consider Implementing cyber security countermeasures at SL 2 for this zone.</div>	

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!



The screenshot shows the ISA website's navigation bar with links for Organizations, Students, About ISA, Feedback, Shopping Cart (0), and Login. The ISA logo and tagline 'Setting the Standard for Automation™' are on the left. Social media icons and a 'Join ISA' button are in the center. A search bar is on the right. Below the navigation bar is a menu with categories: MEMBERSHIP, TRAINING & CERTIFICATIONS, STANDARDS & PUBLICATIONS, CONFERENCES & EVENTS, NEWS & PRESS RELEASES, RESOURCES, TECHNICAL TOPICS, PROFESSIONAL DEVELOPMENT, and STORE.

The main content area displays the breadcrumb trail: Home > Training and Certifications > ISA Training > Instructor-led Training > Assessing the Cybersecurity of New or Existing IACS Systems (IC33). The title 'Assessing the Cybersecurity of New or Existing IACS Systems (IC33)' is prominently displayed. Below the title, the course details are listed: Length: 3 days, CEUs: 2.1, and Certificate Program: Part of the ISA/IEC 62443 Cybersecurity Certificate Program. A red button with the text 'Click here to view all offerings of this course and REGISTER NOW!' is positioned to the right of the course details. The description of the course is provided below the details.

Home > Training and Certifications > ISA Training > Instructor-led Training > Assessing the Cybersecurity of New or Existing IACS Systems (IC33)

Assessing the Cybersecurity of New or Existing IACS Systems (IC33)

Length: 3 days
CEUs: 2.1
Certificate Program: *Part of the ISA/IEC 62443 Cybersecurity Certificate Program*

Your course registration includes your registration for the exam.
Certification of Completion: A Certificate of Completion indicating the total number of CEUs earned will be provided upon successful completion of the course.

Description:

The first phase in the IACS Cybersecurity Lifecycle (defined in ISA 62443-1-1) is to identify and document IACS assets and perform a cybersecurity vulnerability and risk assessment in order to identify and understand the high-risk vulnerabilities that require mitigation. Per ISA 62443-2-1 these assessments need to be performed on both new (i.e. greenfield) and existing (i.e. brownfield) applications. Part of the assessment process involves developing a zone and conduit model of the system, identifying security level targets, and documenting the cybersecurity requirements into a cybersecurity requirements specification (CRS).

Share This Page

- Learn More About Training
- Browse Upcoming Training Offerings
- Download ISA's Training Schedule
- Bring ISA Training To You
- Learn More About Certification
- Learn More About ISA Digital Badges
- Find Testing Windows
- Read a White Paper on Workforce Dev.



Setting the Standard for Automation™

RSA®Conference2019

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/>



Setting the Standard for Automation™

RSAConference2019