S4x20

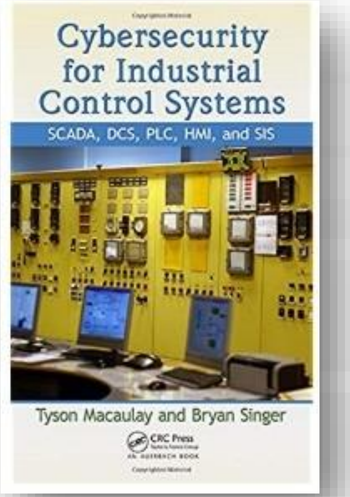
Critical Attack Flow Modeling

Or – why Aquaman sucks…

Bryan L Singer, CISSP, CAP, CAP
Contibutor, Jim McGlone

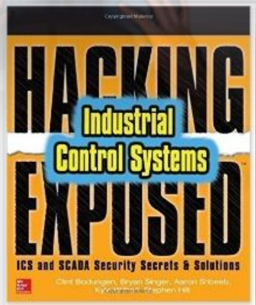
Feb 21, 2020 #S4x20

Presenter Information: Bryan L Singer



- ***Bryan L Singer, CISSP, CAP, CPIN***
  - ***20+ years experience in cybersecurity vulnerability assessments, penetration testing, software design, network performance, network design, ISA-95 integration, security architecture design, incident response and forensics***
  - ***Founding and Past Chair ISA-99/62443***
  - ***Past Director, ISA Safety and Security Division***
  - ***ISA Certified Instructor IC-32, IC-33, IC-34, IC-37, TS-04, TS-12, TS-20***
  - ***Global experience in over 4000 plants***
  - ***Accomplished Red Team Operator and Penetration Test Professional***
  - ***Co-author: Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions***
  - ***Co-author: Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS***

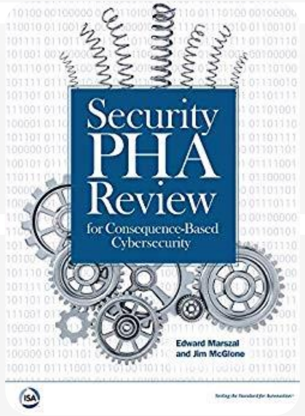
  - ***Recently Joined Accenture: bryan.l.singer@Accenture.com***



Contributor

James McGlone, GICSP

- CMO Kenexis Consulting Corporation
- Co-Author: Security PHA Review for Consequence Based Cybersecurity
- James.mcglone@Kenexis.com



Cybersecurity for OT is an Engineering Problem Requiring an Engineering Solution….

Sound Familiar?

- Security Consultant: I could use this attack to open a valve and cause a rupture…
- Engineer, “Well, I’d just do this…”

….

- <silence>

- So why haven’t you done it?

We Haven’t Connected to the Engineers

Lots of Security "Assessments" and Methodologies

Risk Assessment

HAZOP

Cyber Vulnerability Assessment

Attack Trees

Kill Chains

LOPA

Threat Modeling

CyberPHA

GAP Assessment

PHA

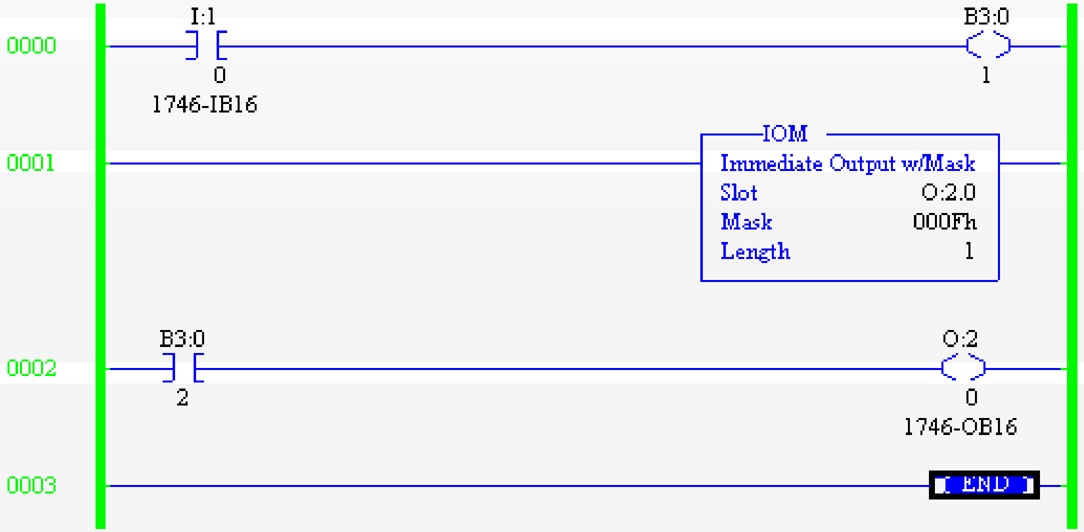
Penetration Test

Challenges to Existing Studies

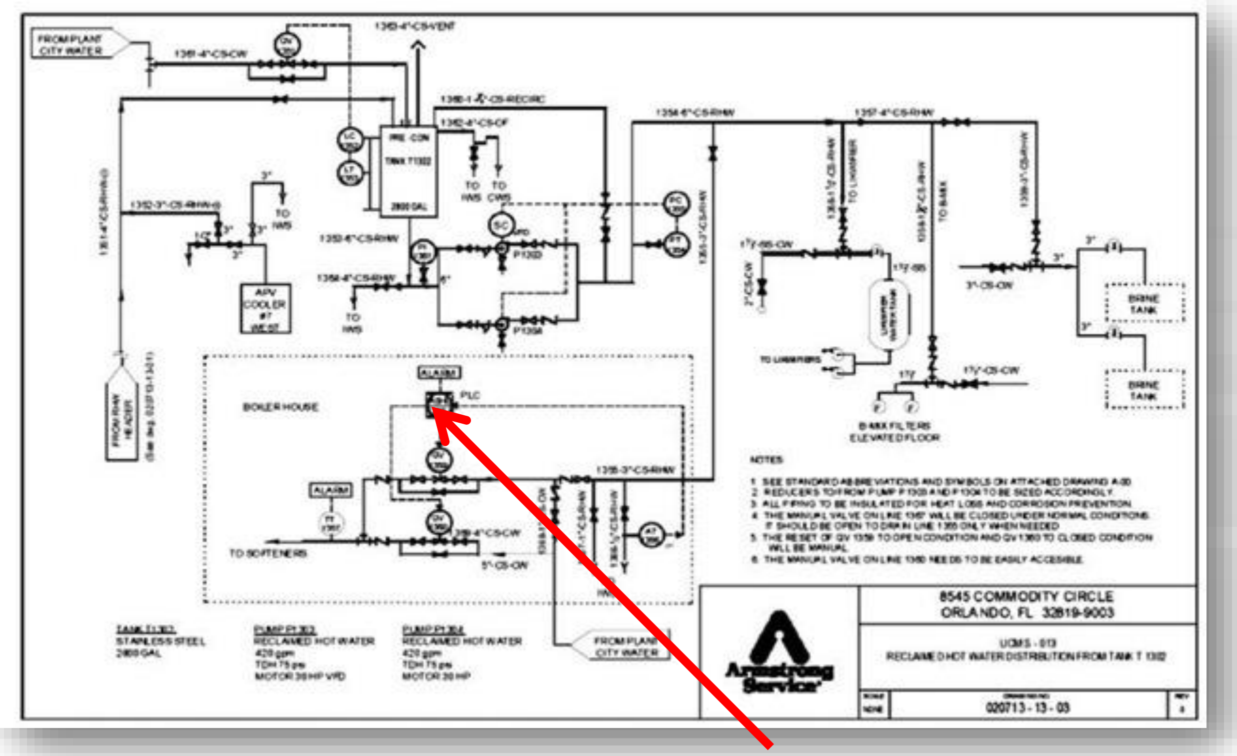
- Too "Static" in nature
- Like Driving a new car off the lot drastically reduces it's value, data is immediately stale
- Often "check the box"
- Don't adequately address cyber-physical controls
- Doesn't naturally create a motivation to action
- Findings not correlated and can increase costs, delay startups, and (as above) don't account for engineering mitigations

Fallacies in ICS Security

- “I’m going to attack the plant at 8:01, and by 8:03, it’s going to go boom”
- “Our Safety Systems will Protect Us”
- “I just found a vulnerability in a control systems, I’m going to blow up a refinery!”



Fundamentally, OT Cyber should be able to answer the question:



What happens if we mess with THIS

Cyber-Physical Security

Safety Standards

- ISA-84
- IEC 61511
- IEC 61508

Cyber Physical Security

Security Standards

- ISO/IEC 27000:2016
- ISA 99/IEC 62443 -
- NIST 800-82

Challenge

Create a Dynamic, Extensible Model and Framework that creates a unified cyber-physical threat model

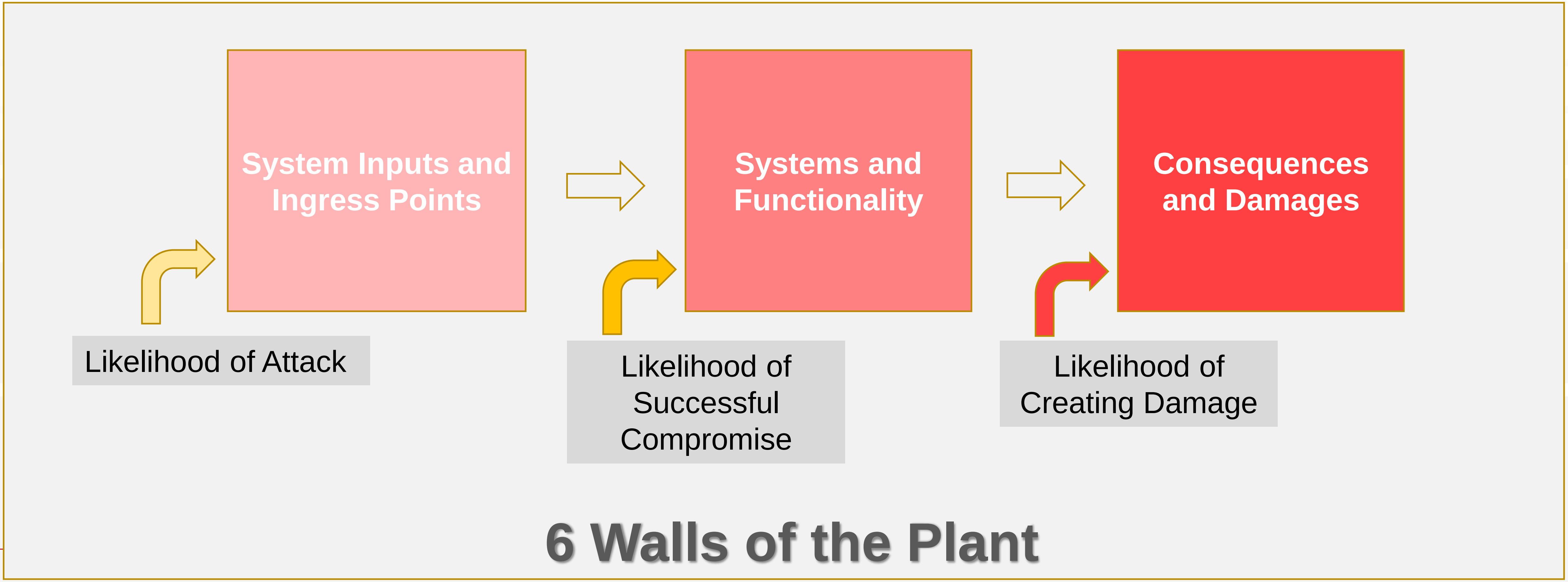
Model should be extensible and dynamically update based on evolving and additional information

Does not replace existing studies or engineering practices, but rather augments and enhances

Should naturally assist in selection of Preventative, Detective, and Reactive Controls

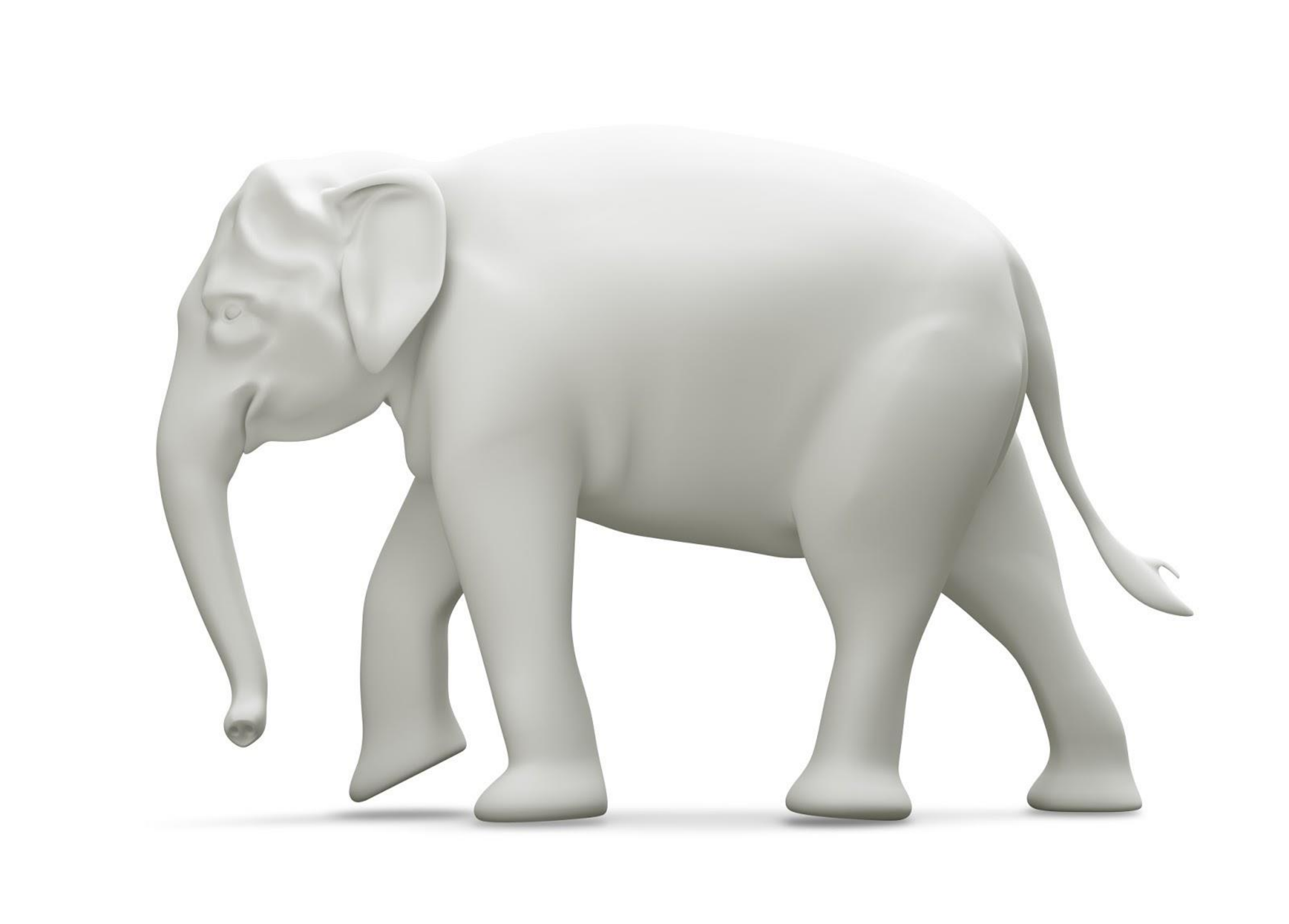
Fundamental Concepts

- Similar to Cyber Kill Chains
- Treats Cybersecurity very much like a supply chain:



Three Key Elements

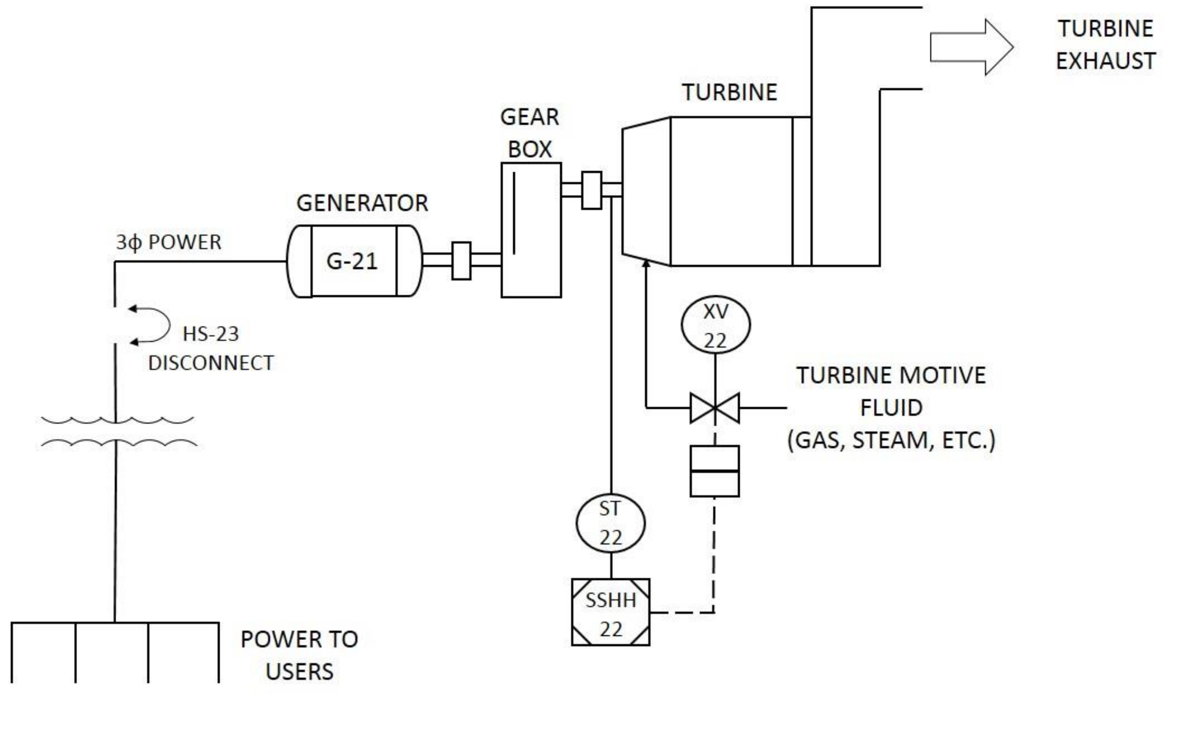
- **Likelihood of exploit for a given system entry point**
  - Based on attack surface, attractiveness of the target, and ease of exploit
- **Likelihood that successful access will result in a successful command and control of a target system**
  - Based on likelihood that attacker will be able to use the system to create a damage scenario
- **Likelihood that successful command and Control will result in a known damage**
  - Factors in engineered safeguards and other protections that could prevent attacker from creating damage
  - Example 1: an attacker can force a valve open, but an emergency relief valve would mitigate damage
  - Example 2: Attacker can close demand and suction valve to a gas compressor, but will not be able to create surge based on machine overspeed protection
  - Example 3: Attacker finds safety builder on digital protection system and interrupts the SIF
  - Example 4: Network or malware based threats are rendered ineffective due to physical controls, but damage scenario can still be created with insider threat, fraud, or collusion

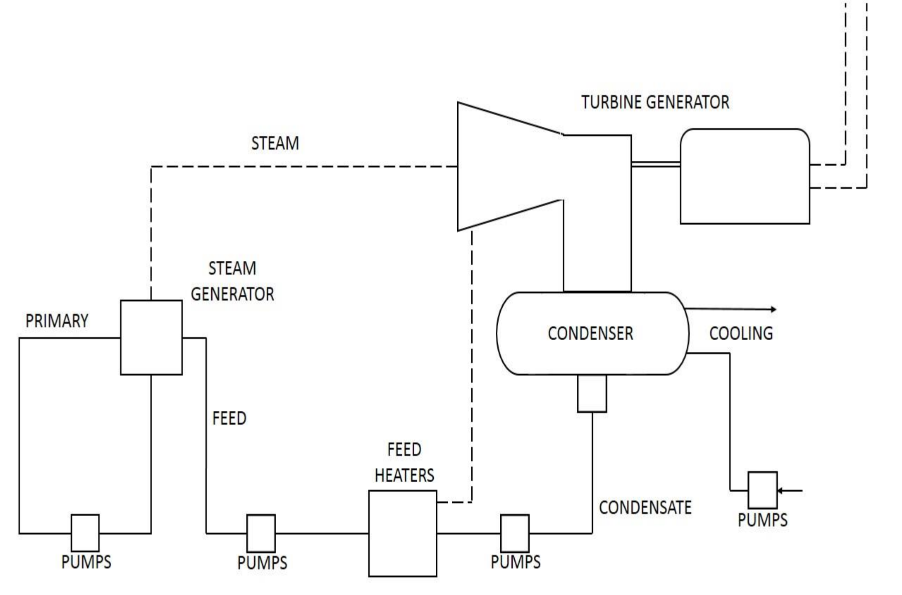


Likelihood is the Aquaman of Cyber Security

(pre Jason Mamoa)

Best Way to Illustrate is by Example…. (very low level)





Go Straight to the Cause and Effect Diagrams

Drawing Title:	SIS Logic Solver Functional Specification	Rev.:	A
Process/Project:	Hydrocracker		
Project Number:			
Tag:	USC-01		
Item Description:	Charge Pump Shutdowns		
Page	Pg 1	of 1	
Client:		By:	

Drawing Number

D67

Rev	Description	Date	By	Approved By
A	For Review			

Output or Effect

Tag	Typ	Act	Equip	Dwg	Description	Action
P-6701A-MS	DO	DEN	P-6701A	D-67-0014	Charge Pump A	STOP
P-6701B-MS	DO	DEN	P-6701B	D-67-0014	Charge Pump B	STOP
XY-676001A	DO	DEN	XV-676001	D-67-0014	Charge Pump Discharge	CLOSE
XY-676001B	DO	DEN	XV-676001	D-67-0014	Charge Pump Discharge	CLOSE
HA-675006	DO	EN	HA-675006	D-67-0013	Reset Alarm Every 5 Minutes	
HL-675004A	DO	EN	HL-675004A	D-67-0014	Charge Pump SD Bypass Light	
HL-675007A	DO	EN	HL-675007A	D-67-0014	Heater SD Bypass Light	
HA-675010	DO	EN	HA-675010	D-67-0014	Reset Alarm Every 5 Minutes	

Input or Cause

Tag	Typ	Act	Description	Dwg	Vote	EULO	EUHI	Units	Trip SP	SC
LT-673005A										X
LT-673005B	AI	LL	Feed Surge Drum	D-67-0013	2oo3	TBD	TBD	TBD	TBD	X
LT-673005C										X
FT-672010A										
FT-672010B	AI	LL	Charge Pump (P-6701A/B) Discharge	D-67-0014	2oo3	TBD	TBD	TBD	TBD	
FT-672010C										
FT-672017A										
FT-672017B	AI	LL	Charge Pump (P-6701A/B) Discharge to Heater	D-67-0014	2oo3	TBD	TBD	TBD	TBD	
FT-672017C										
HS-675003	DI	DEN	Emergency Shutdown	D-67-0014	1oo1	~	~	~	~	
HS-675006	DI	EN	Feed Surge Drum Low Flow SD Maint Bypass	D-67-0013	1oo1	~	~	~	~	
HS-675004	DI	EN	Charge Pump SD Bypass Switch	D-67-0014	1oo1	~	~	~	~	
HS-675007	DI	EN	Heater SD Bypass Switch	D-67-0014	1oo1	~	~	~	~	
HS-675010	DI	EN	Hydrocarbon to Htr Low Flow SD Maint Bypass	D-67-0014	1oo1	~	~	~	~	
HS-675005	DI	EN	Reset	D-67-0014	1oo1	~	~	~	~	
ZSO-675030	DI	DEN	Charge Pump (P-6701A) Inlet ZSO	D-67-0014	1oo1	~	~	~	~	
ZSC-675030	DI	DEN	Charge Pump (P-6701A) Inlet ZSC	D-67-0014	1oo1	~	~	~	~	
ZSO-675031	DI	DEN	Charge Pump (P-6701B) Inlet ZSO	D-67-0014	1oo1	~	~	~	~	
ZSC-675031	DI	DEN	Charge Pump (P-6701B) Inlet ZSC	D-67-0014	1oo1	~	~	~	~	
ZSO-676001	DI	DEN	Charge Pump (P-6701A/B) Discharge ZSO	D-67-0014	1oo1	~	~	~	~	
ZSC-676001	DI	DEN	Charge Pump (P-6701A/B) Discharge ZSC	D-67-0014	1oo1	~	~	~	~	

- Is there a cyber component that would allow a C&E listed event to be realized?
- How difficult is it to gain access to this control?
- What mitigating cyber controls exist?
- What detective controls exist?
- What engineered safeguards exist?

Attack Flow Models – Change Likelihood of Compromise

Attack Flow	Point of Entry	Likelihood of Exploit	System Accessed	Consequence(s)	Ease of Exploit	Risk of Loss/Damage	Consequence Exposure	Raw Exposure	Risk
1	HMI, RDP Session	38%	Valve Control System	Force Valve Open	65%	$ 2,000,000	60%	$ 1,200,000.0	$296,400
				Force Valve Closed	65%	$ 2,000,000	60%	$ 1,200,000.0	$296,400
				Report False Valve State	35%	$ 2,000,000	20%	$ 400,000.0	$53,200
2	HMI Spoofing Control Protocols	10%	Valve Control System	Force Valve Open	5%	$ 2,000,000	85%	$ 1,700,000.0	$8,500
				Force Valve Closed	5%	$ 2,000,000	85%	$ 1,700,000.0	$8,500
				Report False Valve State	35%	$ 2,000,000	35%	$ 700,000.0	$24,500

Attack Flow	Point of Entry	Likelihood of Exploit	System Accessed	Consequence(s)	Ease of Exploit	Risk of Loss/Damage	Consequence Exposure	Raw Exposure	Risk	Delta
1	HMI, RDP Session	65%	Valve Control System	Force Valve Open	65%	$ 2,000,000	60%	$ 1,200,000.0	$507,000	$210,600
				Force Valve Closed	65%	$ 2,000,000	60%	$ 1,200,000.0	$507,000	$210,600
				Report False Valve State	35%	$ 2,000,000	20%	$ 400,000.0	$91,000	$37,800
2	HMI Spoofing Control Protocols	35%	Valve Control System	Force Valve Open	5%	$ 2,000,000	85%	$ 1,700,000.0	$55,250	$55,250
				Force Valve Closed	5%	$ 2,000,000	85%	$ 1,700,000.0	$55,250	$46,750
				Report False Valve State	35%	$ 2,000,000	35%	$ 700,000.0	$159,250	$150,750

Attack Flow – Change Ease of Exploit / Likelihood of Creating Damage

Attack Flow	Point of Entry	Likelihood of Exploit	System Accessed	Consequence(s)	Ease of Exploit	Risk of Loss/Damage	Consequence Exposure	Raw Exposure	Risk	Delta
1	HMI, RDP Session	65%	Valve Control System	Force Valve Open	85%	$ 2,000,000	60%	$ 1,200,000.0	$663,000	$366,600
				Force Valve Closed	85%	$ 2,000,000	60%	$ 1,200,000.0	$663,000	$366,600
				Report False Valve State	45%	$ 2,000,000	20%	$ 400,000.0	$117,000	$63,800
2	HMI Spoofing Control Protocols	35%	Valve Control System	Force Valve Open	15%	$ 2,000,000	85%	$ 1,700,000.0	$165,750	$165,750
				Force Valve Closed	15%	$ 2,000,000	85%	$ 1,700,000.0	$165,750	$157,250
				Report False Valve State	40%	$ 2,000,000	35%	$ 700,000.0	$182,000	$173,500

Attack Flow	Point of Entry	Likelihood of Exploit	System Accessed	Consequence(s)	Ease of Exploit	Risk of Loss/Damage	Consequence Exposure	Raw Exposure	Risk	Delta
1	HMI, RDP Session	5%	Valve Control System	Force Valve Open	65%	$ 2,000,000	60%	$ 1,200,000.0	$39,000	($257,400)
				Force Valve Closed	65%	$ 2,000,000	60%	$ 1,200,000.0	$39,000	($257,400)
				Report False Valve State	35%	$ 2,000,000	20%	$ 400,000.0	$7,000	($46,200)
2	HMI Spoofing Control Protocols	15%	Valve Control System	Force Valve Open	5%	$ 2,000,000	85%	$ 1,700,000.0	$4,250	$4,250
				Force Valve Closed	5%	$ 2,000,000	85%	$ 1,700,000.0	$4,250	($4,250)
				Report False Valve State	30%	$ 2,000,000	35%	$ 700,000.0	$10,500	$2,000

- Dealing with the White Elephant … or …

Turning Likelihood into Your Greatest Ally

20+ Years of Consulting Has Taught Me to Turn Your Biggest Impediments into Your Greatest Strength

Challenge	Risk	Action
Customer Cannot Supply Accurate Documentation	• Errors and Omissions • Inaccurate Findings • False Positives	Turn accuracy of collected data into a finding in the report
Inaccurate or Missing Architecture Diagrams	• Unintended System Impacts • Incomplete Findings	Demonstrate to customer how long an incident response would take at their current level of accuracy versus fully accurate
Customer takes 8 hours to correctly turn up a SPAN/Monitor Report	• Not enough data for analysis • Inaccurate Analysis • Greater chance periodic beaconing malware is missed	Demonstrate how this time gap could result in extended problems during a cyber event

Evolving Likelihood Into a Strength

Sample Categories	Analysis	Resulting Controls
MITRE ATT&CK Event ID's	• Identify MITRE Attack Paths and Corresponding Event ID's Likely to be used in Attack	• Create detection rules for occurrence of these event ID's in Windows Logs • Correlate the occurrence of these event ID's to network PCAP to identify possible attack • Enhance IR and Forensics by providing enhanced time windows to hunt for attack
Attack Surface	• Determine porosity of the attack surface by ports/services • Enhance data with vulnerability scanning	• Better justification for patching • Adopt detective controls in IDS or SIEM for devices that cannot be readily mitigated
Attractiveness of the Target	• Leverage military analogies of high value versus high payoff targets and the overall attractiveness to attackers • Enhance this data through IDS logs, honeypots, honeynets, and other threat data	• Helpful in identifying which systems would be most likely for exploit • Can be evolved over time based on changing threat landscape
Identify Mitigating Cyber Controls	• Identify mitigating controls such as blocking port 445 and reducing likelihood of ransomware	• Where physical controls cannot be immediately enhanced, provide better cyber preventative and detective controls • Help justify network and security upgrades based on realistic cyberphysical threat data
Identify Mitigating Engineered Safeguards	• Identify if a fundamentally unhackable physical control can or does mitigate the cyber threat	• Identify strategies to mitigate cyber threat while simultaneously identifying where incidents of fraud, collusion, or insider threat could impact operations

Equipment	Vulnerability Aspects			Scenario Notes	Affected Industries
	Susceptibility	Severity	Aggregate		
Boiler	Very High	High	Yes	Drain steam drum, allow to heat up, rapidly re-introduce water, resulting in steam explosion. Disable shutdowns and Alarms. Override safety devices and energize fuel valves to idle boiler.	Power Generation, Pulp & Paper, Chemical
Pressure Vessels	Moderate	Moderate	Unlikely	Change in Operating Conditions and override safety devices. Most likely not an issue due to mechanical protection, but several instances of hazardous chemical reaction/decomposition due to change in process conditions.	Chemical
Furnace / Oven / Kilns	Moderate	Moderate	Unlikely	Open fuel gas to idle heater. Allow ambient ignition sources, or create ignition with automatic igniter.	General Manufacturing, Pulp & Paper, Chemical
Gas Compressor	Moderate	Moderate	Unlikely	Bypass safety devices and initiate demand by blocked suction, blocked discharge, recirculation without cooling, introduce liquid, etc.	Chemical
Gas Turbines	High	Moderate	Yes	Override electronic overspeed shutdown and disconnect load.	Power Generation
Steam Turbines	High	Moderate	Yes	Override electronic overspeed shutdown and disconnect load.	Power Generation
Generators	High	Moderate	Yes	Override electronic overspeed shutdown and disconnect load.	Power Generation
Power Transformers	Low	Low	No	Limited Automation	Power Generation, General Manufacturing

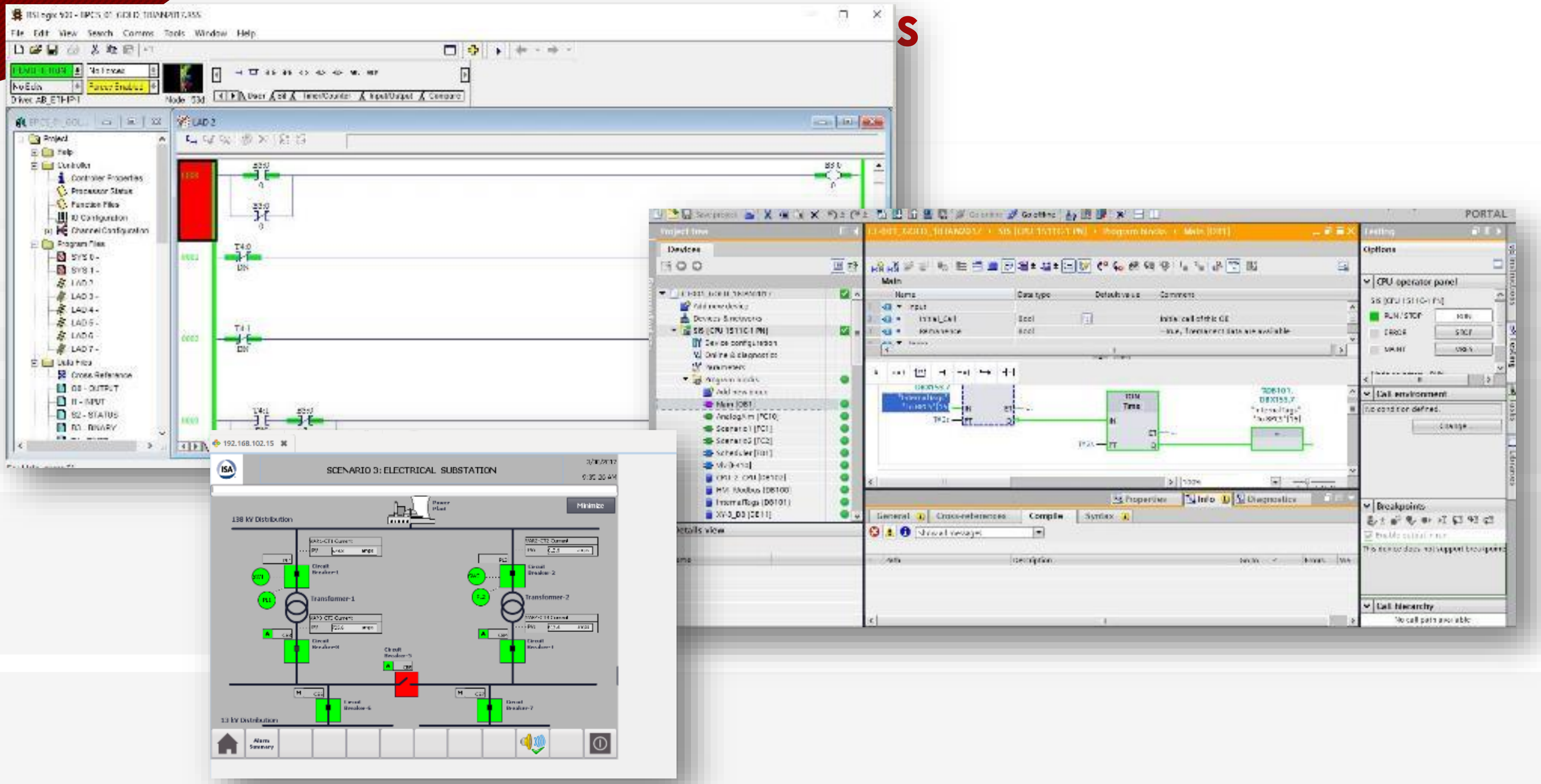
Outputs from This Approach

Methods of Calculating Likelihood

Sample Outputs

- PCAP from a Partial Stroke Test turned into an IDS rule and alert
- Mitre ATT&CK Event ID's and correlation engine to Windows System Events and PCAPs for SIEM Integration
- Writing DPI rules in firewalls to check for particular MODBUS coil and register access from valid IP addresses, VLAN's, and control devices
- Identifying additional engineered safeguards to mitigate specific attack flows

S



SCENARIO 3: ELECTRICAL SUBSTATION
138 kV Distribution
13 kV Distribution
PORTAL

Questions

Name

Phone

Email

Website

Customize this Template

[Template Editing Instructions and Feedback]