CyberPHA

A proven method to assess industrial control system cybersecurity risk

Presented by: Jacob Morella

John A. Cusimano

Vice President of Industrial Cybersecurity

aeSolutions

John.Cusimano@aesolns.com

- 30 years experience in industrial automation
    - Kodak, Moore Products, Siemens, exida, aeSolutions
- Specialization in:
    - ICS Cybersecurity
    - Process Safety
    - Safety Instrumented Systems
    - High-availability systems
    - Industrial Networking
- ISA 99 voting member since 2009
- Chairman of recently approved ISA 62443-3-2 standard
- Lead developer/instructor for ISA cybersecurity training

Jacob Morella, PE$_{(SC)}$

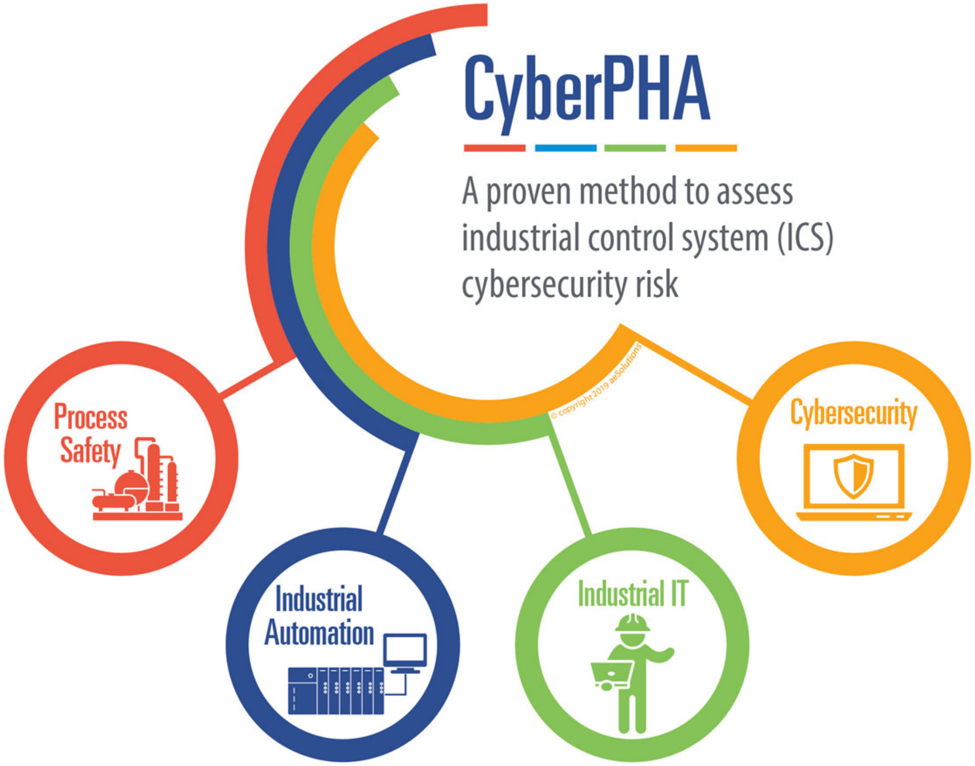
Industrial Cybersecurity Technical Project Manager

aeSolutions

Jacob.Morella@aesolns.com

- Experience in the process and process safety industries
  - Process/Production Engineer
  - PHA, LOPA, and Alarm Rationalization Facilitator
  - Automation Engineer
- Specialization in:
  - ICS Cybersecurity
  - Process Safety
  - Safety Instrumented Systems
- ISA cybersecurity trainer
- PHA/LOPA Trainer

A CyberPHA Is



CyberPHA

A proven method to assess industrial control system (ICS) cybersecurity risk

Process Safety

Industrial Automation

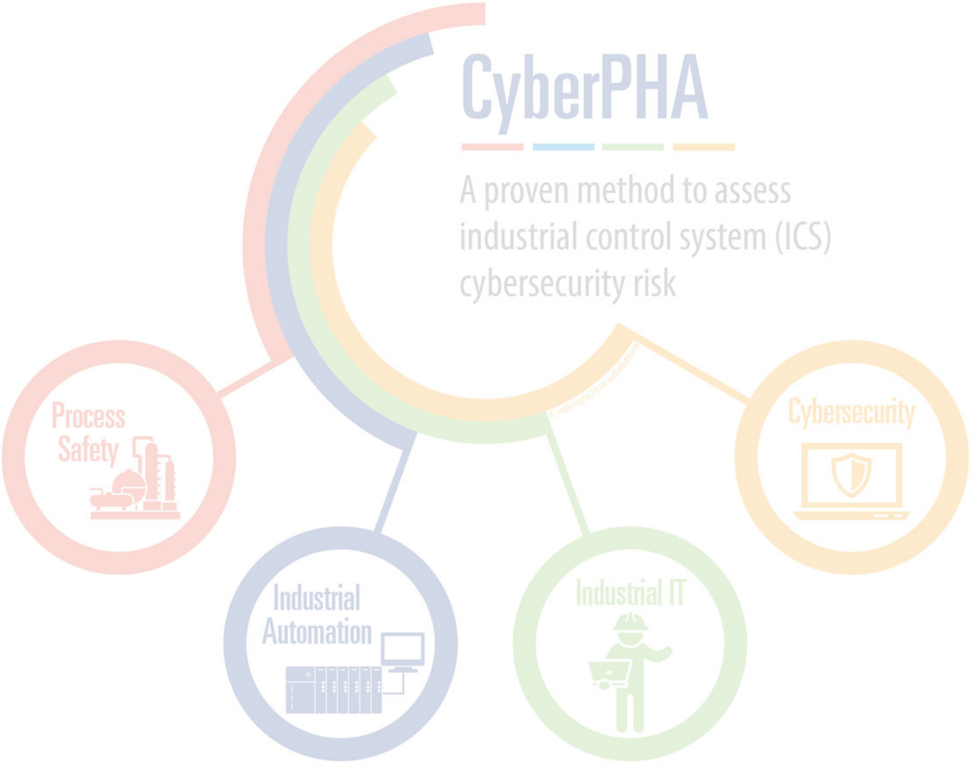
Industrial IT

Cybersecurity

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

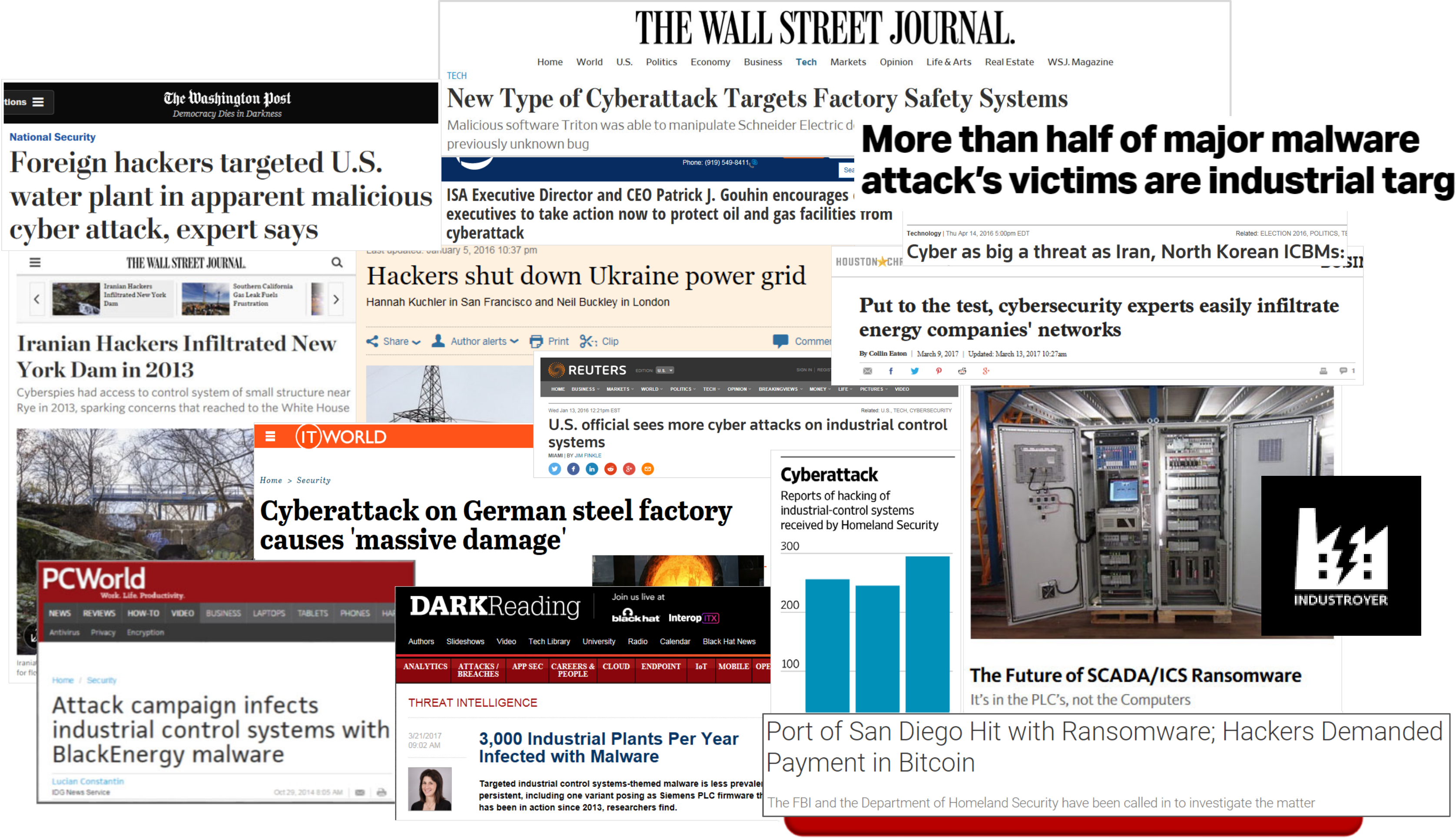
- Systematic, consequence-driven approach
- Aligned with ISA/IEC 62443-3-2 and ISA TR84.00.09 standards
- Leverages established process safety information and techniques (e.g. PHA/HAZOP/LOPA)
- Integrates multiple engineering disciplines
- Delivers a risk-ranked mitigation plan

A CyberPHA Is


CyberPHA
A proven method to assess industrial control system (ICS) cybersecurity risk
Process Safety
Industrial Automation
Industrial IT
Cybersecurity

- Not a way to assign blame
- Not a solo activity
- Not an Audit
- **Not a replacement for Process Safety PHAs**

It’s not just about IT anymore - Operations is a target



THE WALL STREET JOURNAL.

TECH

New Type of Cyberattack Targets Factory Safety Systems

Malicious software Triton was able to manipulate Schneider Electric d
previously unknown bug

The Washington Post
Democracy Dies in Darkness

National Security

Foreign hackers targeted U.S. water plant in apparent malicious cyber attack, expert says

ISA Executive Director and CEO Patrick J. Gouhin encourages executives to take action now to protect oil and gas facilities from cyberattack

More than half of major malware attack’s victims are industrial targets

Technology | Thu Apr 14, 2016 5:00pm EDT
Related: ELECTION 2016, POLITICS, TE

Cyber as big a threat as Iran, North Korean ICBMs:

THE WALL STREET JOURNAL.

Iranian Hackers Infiltrated New York Dam
Southern California Gas Leak Fuels Frustration

Iranian Hackers Infiltrated New York Dam in 2013

Cyberspies had access to control system of small structure near Rye in 2013, sparking concerns that reached to the White House

Last updated: January 5, 2016 10:37 pm

Hackers shut down Ukraine power grid

Hannah Kuchler in San Francisco and Neil Buckley in London

HOUSTON CHRONICLE

Put to the test, cybersecurity experts easily infiltrate energy companies' networks

By Collin Eaton | March 9, 2017 | Updated: March 13, 2017 10:27am

REUTERS

Wed Jan 13, 2016 12:21pm EST
Related: U.S., TECH, CYBERSECURITY

U.S. official sees more cyber attacks on industrial control systems

MIAMI | BY JIM FINKLE

IT WORLD

Home > Security

Cyberattack on German steel factory causes 'massive damage'

Cyberattack

Reports of hacking of industrial-control systems received by Homeland Security

INDUSTROYER

The Future of SCADA/ICS Ransomware

It’s in the PLC’s, not the Computers

PCWorld
Work. Life. Productivity.

Home / Security

Attack campaign infects industrial control systems with BlackEnergy malware

Lucian Constantin
IDG News Service
Oct 29, 2014 8:05 AM

DARKReading
Join us live at black hat Interop ITX

THREAT INTELLIGENCE

3/21/2017
09:02 AM

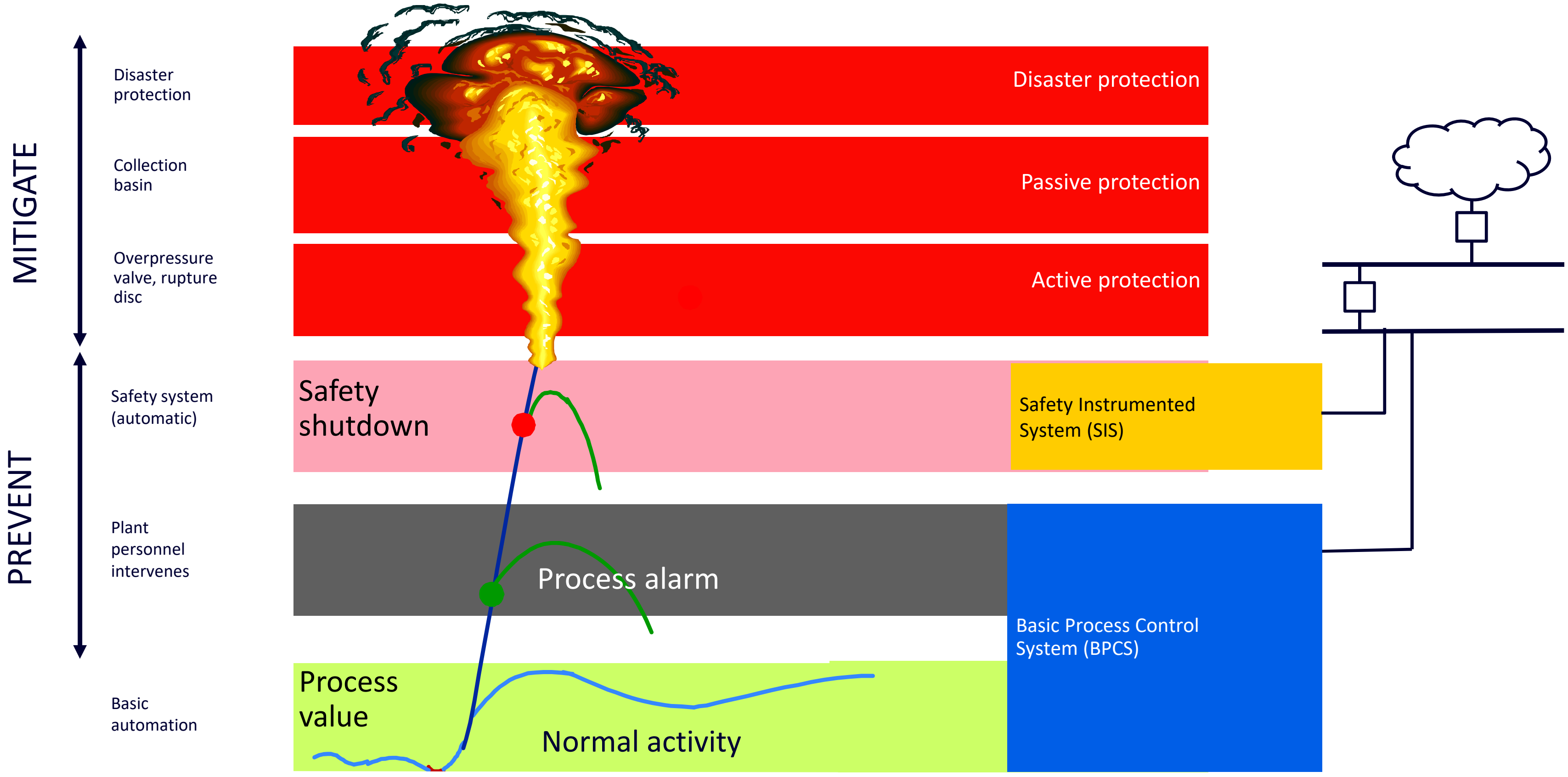
3,000 Industrial Plants Per Year Infected with Malware

Targeted industrial control systems-themed malware is less prevale persistent, including one variant posing as Siemens PLC firmware th has been in action since 2013, researchers find.

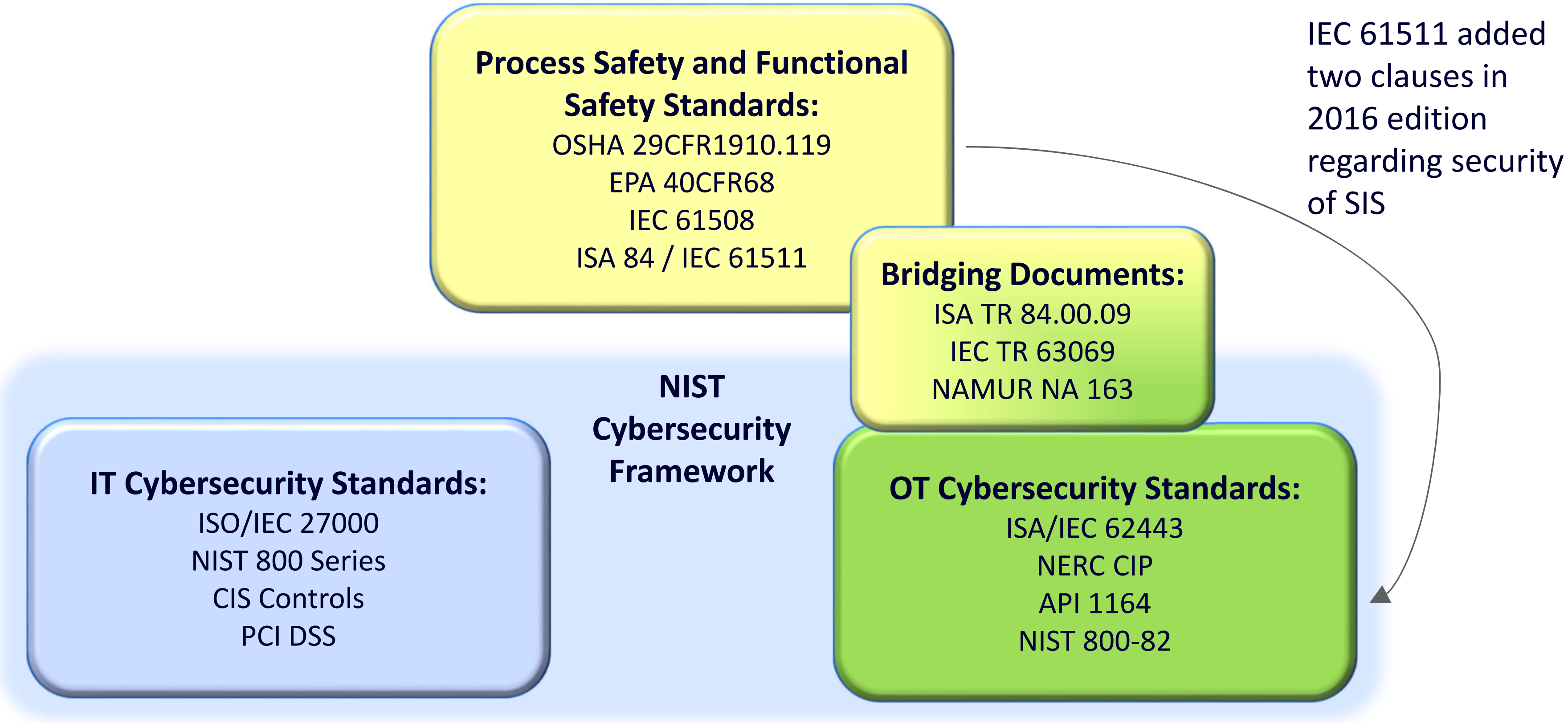
Port of San Diego Hit with Ransomware; Hackers Demanded Payment in Bitcoin

The FBI and the Department of Homeland Security have been called in to investigate the matter

Process Safety & Industrial Cybersecurity



Process Safety & Cybersecurity Standards



Process Safety and Functional Safety Standards:
OSHA 29CFR1910.119
EPA 40CFR68
IEC 61508
ISA 84 / IEC 61511

Bridging Documents:
ISA TR 84.00.09
IEC TR 63069
NAMUR NA 163

NIST Cybersecurity Framework

IT Cybersecurity Standards:
ISO/IEC 27000
NIST 800 Series
CIS Controls
PCI DSS

OT Cybersecurity Standards:
ISA/IEC 62443
NERC CIP
API 1164
NIST 800-82

IEC 61511 added two clauses in 2016 edition regarding security of SIS

Functional Safety Standards

INTERNATIONAL STANDARD

IEC 61511-1

First edition
2003-01

Functional safety –
Safety instrumented systems
for the process industry sector –

Part 1:
Framework, definitions, system,
hardware and software requirements

Sécurité fonctionnelle –
Systèmes instrumentés de sécurité pour le secteur
des industries de transformation –

Partie 1:
Cadre, définitions et prescriptions concernant
le système,
le matériel et le logiciel

Ref ce number
IEC 61 1:2003(E)

61511-1 2nd Edition, FDIS

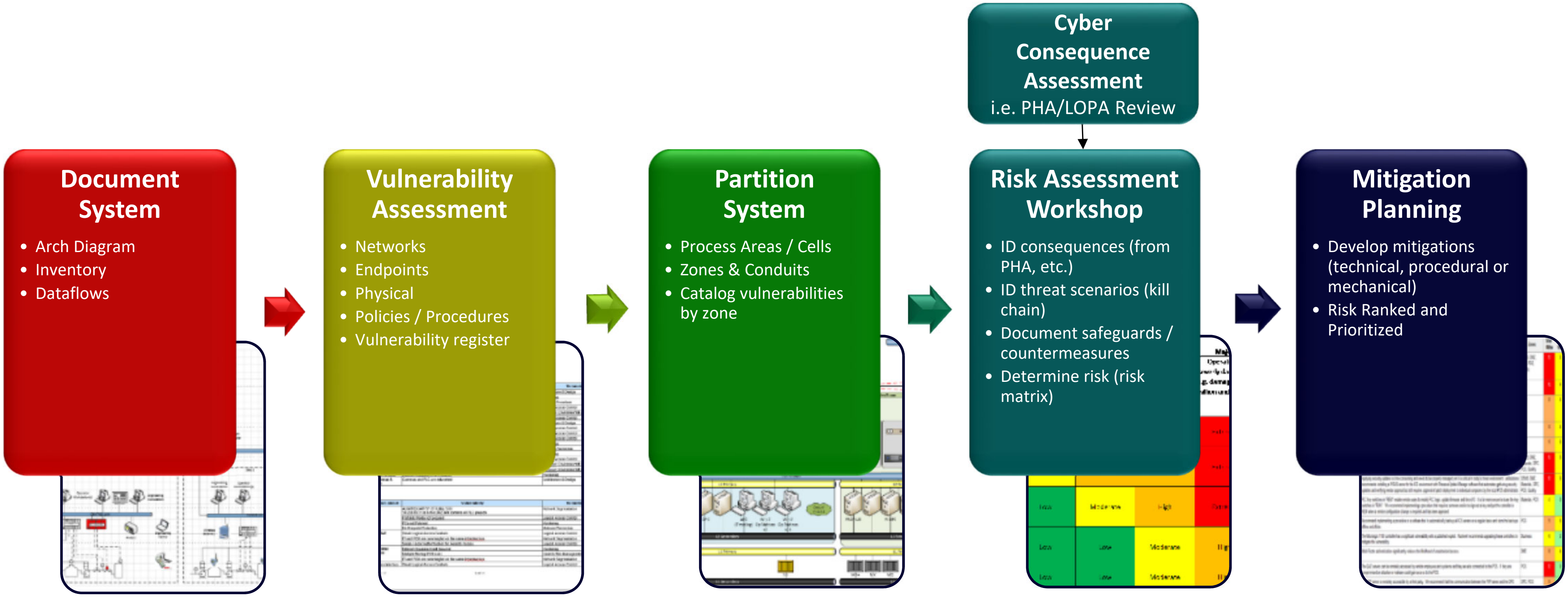
- 8.2.4: A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS
- 11.2.12: The design of the SIS shall be such that it provides the necessary resilience against the identified security risks

NOTE: Guidance related to SIS security is provided in ISA TR84.00.09 and ISA/IEC 62443-3-2.

Cyber Risk Assessment Challenges

- Modern control systems and safety systems are complex
- It very common for them to be integrated
- A single threat or vulnerability could disable multiple layers of protection
- Identifying the cyber threats and vulnerabilities that can lead to high risk consequences can be challenging
- Process safety studies (e.g. PHAs, HAZOPs, LOPAs) typically do not take into account cybersecurity initiating events or effectiveness of cybersecurity safeguards

The CyberPHA Process



Cyber Consequence Assessment
i.e. PHA/LOPA Review

Document System

- Arch Diagram
- Inventory
- Dataflows

Vulnerability Assessment

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

Partition System

- Process Areas / Cells
- Zones & Conduits
- Catalog vulnerabilities by zone

Risk Assessment Workshop

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

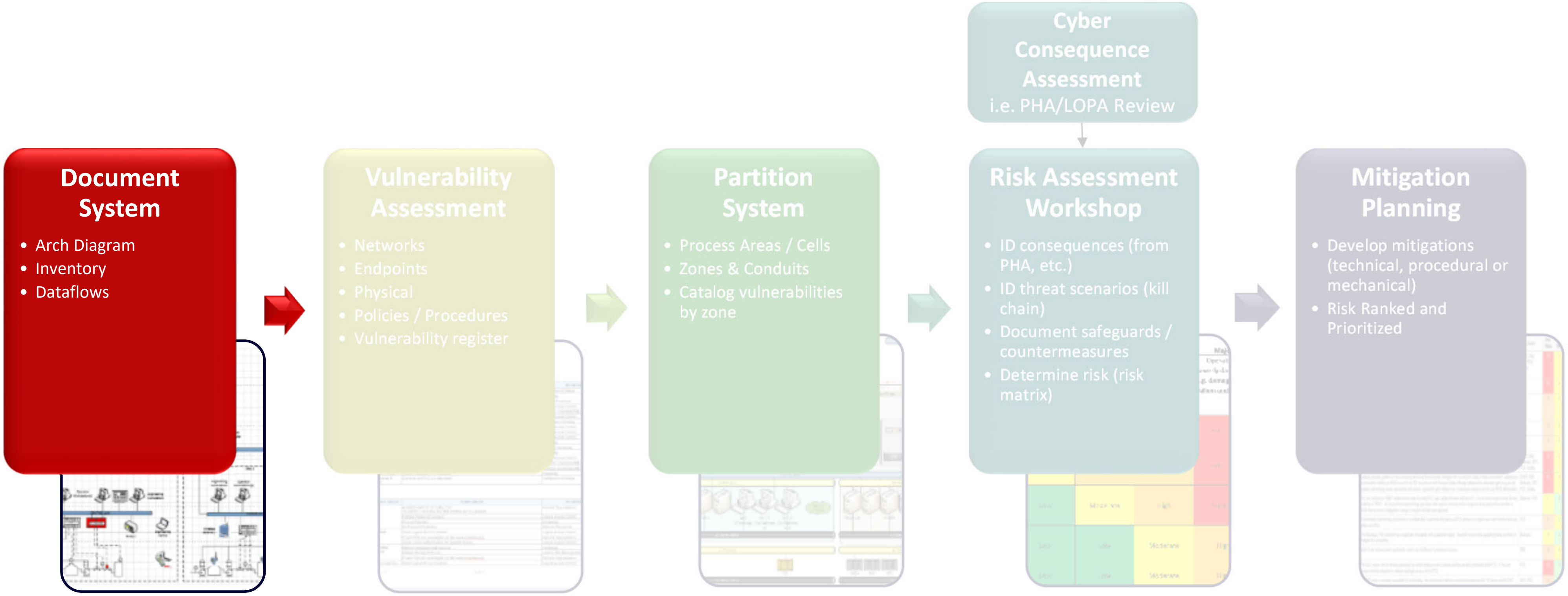
Mitigation Planning

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

CyberPHA Benefits

- Provides management with risk-ranked mitigation plan
- Encourages collaboration, practical solutions and buy-in
- Satisfies new IEC 61511 SIS security requirements
- Uncovers “hidden” risks
- Establishes a baseline to measure progress and justify decisions
- Raises cybersecurity awareness
- Successfully applied to hundreds of ICS since 2013

The CyberPHA Process



Document System

- Arch Diagram
- Inventory
- Dataflows

Vulnerability Assessment

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

Partition System

- Process Areas / Cells
- Zones & Conduits
- Catalog vulnerabilities by zone

Cyber Consequence Assessment

i.e. PHA/LOPA Review

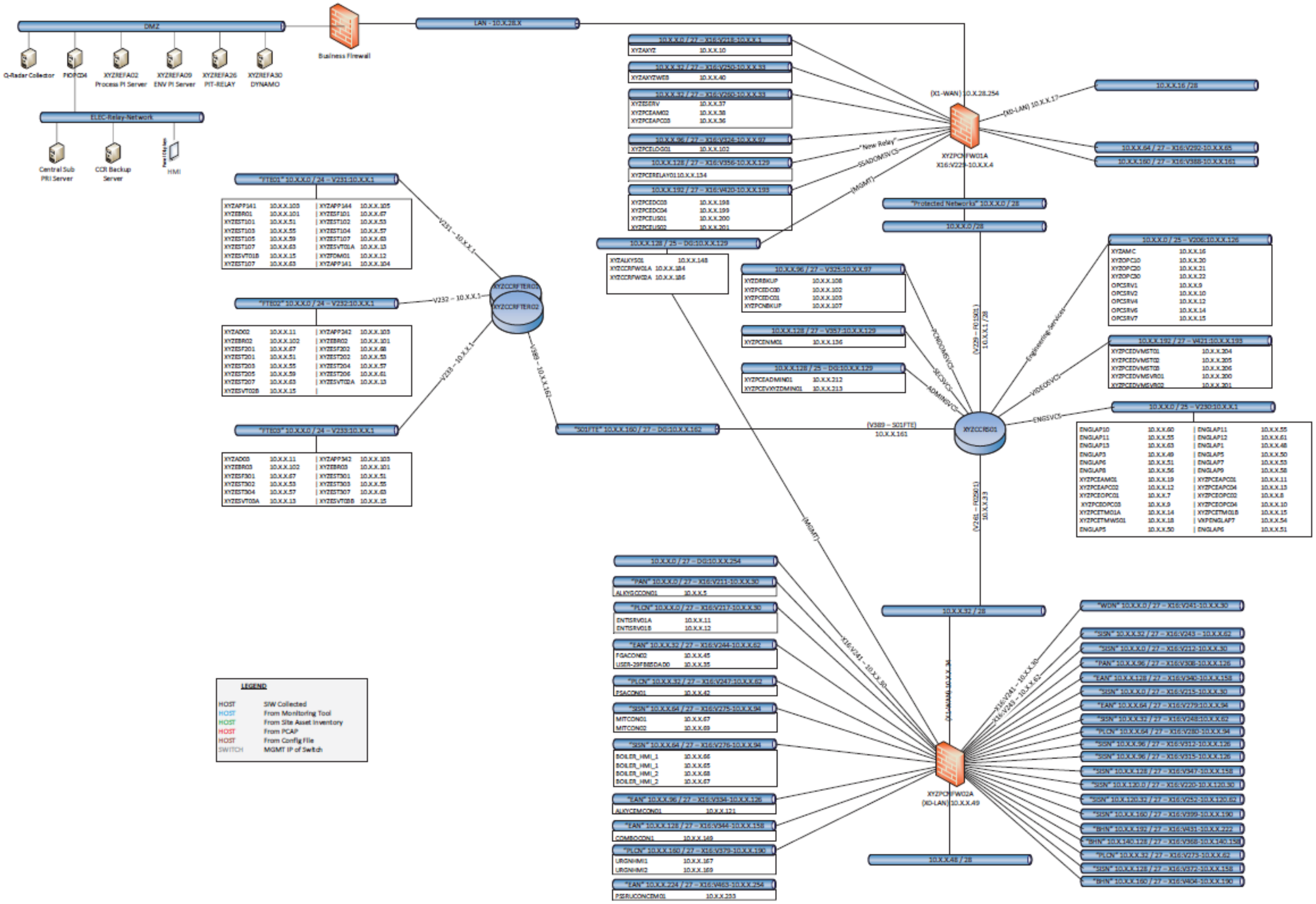
Risk Assessment Workshop

- 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

Example “As-Found” Logical Network Diagram


DMZ
Q-Radar Collector
PIOPC04
XYZREFA02
Process PI Server
XYZREFA09
ENV PI Server
XYZREFA26
PIT-RELAY
XYZREFA30
DYNAMO
Business Firewall
LAN - 10.X.28.X
ELEC-Relay-Network
Central Sub
PRI Server
CCR Backup
Server
HMI
10.X.X.0 / 27 – X16:V218-10.X.X.1
10.X.X.32 / 27 – X16:V250-10.X.X.33
10.X.X.32 / 27 – X16:V260-10.X.X.33
10.X.X.96 / 27 – X16:V324-10.X.X.97
10.X.X.128 / 27 – X16:V356-10.X.X.129
10.X.X.192 / 27 – X16:V420-10.X.X.193
10.X.X.128 / 25 – DG:10.X.X.129
“New Relay”
SSADOMSVCS
(MGMT)
(X1-WAN) 10.X.28.254
(X0-LAN) 10.X.X.17
XYZPCNFW01A
X16:V229-10.X.X.4
10.X.X.16 /28
10.X.X.64 / 27 – X16:V292-10.X.X.65
10.X.X.160 / 27 – X16:V388-10.X.X.161
“Protected Networks” 10.X.X.0 / 28
10.X.X.0 /28
“FTE01” 10.X.X.0 / 24 – V231:10.X.X.1
“FTE02” 10.X.X.0 / 24 – V232:10.X.X.1
“FTE03” 10.X.X.0 / 24 – V233:10.X.X.1
V231 – 10.X.X.1
V232 – 10.X.X.1
V233 – 10.X.X.1
XYZCCRFTER01
XYZCCRFTER02
V389 – 10.X.X.162
“S01FTE” 10.X.X.160 / 27 – DG:10.X.X.162
(V389 – S01FTE)
10.X.X.161
10.X.X.96 / 27 – V325:10.X.X.97
10.X.X.128 / 27 – V357:10.X.X.129
10.X.X.128 / 25 – DG:10.X.X.129
PCNDOMSVCS
SECSVCS
ADMINSVCS
(V229 – F01S01)
10.X.X.1 /28
Engineering Services
VIDEOSVCS
ENGSVCS
XYZCCRS01
10.X.X.0 / 25 – V206:10.X.X.126
10.X.X.192 / 27 – V421:10.X.X.193
10.X.X.0 / 25 – V230:10.X.X.1
(V261 – F02S01)
10.X.X.33
(MGMT)
10.X.X.32 / 28
X16:V241 – 10.X.X.30
X16:V241 – 10.X.X.30
X16:V243 – 10.X.X.62
(X1-WAN) 10.X.X.34
XYZPCNFW02A
(X0-LAN) 10.X.X.49
10.X.X.48 / 28
10.X.X.0 / 27 – DG:10.X.X.254
“PAN” 10.X.X.0 / 27 – X16:V211-10.X.X.30
“PLCN” 10.X.X.0 / 27 – X16:V217-10.X.X.30
“EAN” 10.X.X.32 / 27 – X16:V244-10.X.X.62
“PLCN” 10.X.X.32 / 27 – X16:V247-10.X.X.62
“SISN” 10.X.X.64 / 27 – X16:V275-10.X.X.94
“SISN” 10.X.X.64 / 27 – X16:V276-10.X.X.94
“EAN” 10.X.X.96 / 27 – X16:V334-10.X.X.126
“EAN” 10.X.X.128 / 27 – X16:V344-10.X.X.158
“PLCN” 10.X.X.160 / 27 – X16:V379-10.X.X.190
“EAN” 10.X.X.224 / 27 – X16:V463-10.X.X.254
“WDN” 10.X.X.0 / 27 – X16:V241-10.X.X.30
“SISN” 10.X.X.32 / 27 – X16:V243 – 10.X.X.62
“SISN” 10.X.X.0 / 27 – X16:V212-10.X.X.30
“PAN” 10.X.X.96 / 27 – X16:V308-10.X.X.126
“EAN” 10.X.X.128 / 27 – X16:V340-10.X.X.158
“SISN” 10.X.X.0 / 27 – X16:V215-10.X.X.30
“EAN” 10.X.X.64 / 27 – X16:V279-10.X.X.94
“SISN” 10.X.X.32 / 27 – X16:V248-10.X.X.62
“PLCN” 10.X.X.64 / 27 – X16:V280-10.X.X.94
“SISN” 10.X.X.96 / 27 – X16:V312-10.X.X.126
“SISN” 10.X.X.96 / 27 – X16:V315-10.X.X.126
“SISN” 10.X.X.128 / 27 – X16:V347-10.X.X.158
“SISN” 10.X.120.0 / 27 – X16:V220-10.X.120.30
“SISN” 10.X.120.32 / 27 – X16:V252-10.X.120.62
“SISN” 10.X.X.160 / 27 – X16:V399-10.X.X.190
“BHN” 10.X.X.192 / 27 – X16:V431-10.X.X.222
“BHN” 10.X.140.128 / 27 – X16:V368-10.X.140.158
“PLCN” 10.X.X.32 / 27 – X16:V273-10.X.X.62
“SISN” 10.X.X.128 / 27 – X16:V372-10.X.X.158
“BHN” 10.X.X.160 / 27 – X16:V404-10.X.X.190

XYZAPP141	10.X.X.103	XYZAPP144	10.X.X.105
XYZEBR01	10.X.X.101	XYZESF101	10.X.X.67
XYZEST101	10.X.X.51	XYZEST102	10.X.X.53
XYZEST103	10.X.X.55	XYZEST104	10.X.X.57
XYZEST105	10.X.X.59	XYZEST107	10.X.X.63
XYZEST107	10.X.X.63	XYZESVT01A	10.X.X.13
XYZESVT01B	10.X.X.15	XYZFDM01	10.X.X.12
XYZEST107	10.X.X.63	XYZAPP141	10.X.X.104

XYZAD02	10.X.X.11	XYZAPP242	10.X.X.103
XYZEBR02	10.X.X.102	XYZEBR02	10.X.X.101
XYZESF201	10.X.X.67	XYZESF202	10.X.X.68
XYZEST201	10.X.X.51	XYZEST202	10.X.X.53
XYZEST203	10.X.X.55	XYZEST204	10.X.X.57
XYZEST205	10.X.X.59	XYZEST206	10.X.X.61
XYZEST207	10.X.X.63	XYZESVT02A	10.X.X.13
XYZESVT02B	10.X.X.15		

XYZAD03	10.X.X.11	XYZAPP342	10.X.X.103
XYZEBR03	10.X.X.102	XYZEBR03	10.X.X.101
XYZESF301	10.X.X.67	XYZEST301	10.X.X.51
XYZEST302	10.X.X.53	XYZEST303	10.X.X.55
XYZEST304	10.X.X.57	XYZEST307	10.X.X.63
XYZESVT03A	10.X.X.13	XYZESVT03B	10.X.X.15

XYZAXYZ	10.X.X.10

XYZAXYZWEB	10.X.X.40

XYZESERV	10.X.X.37
XYZPCEAM02	10.X.X.38
XYZPCEAPC03	10.X.X.36

XYZPCELOG01	10.X.X.102

XYZPCERELAY01	10.X.X.134

XYZPCEDC03	10.X.X.198
XYZPCEDC04	10.X.X.199
XYZPCEUS01	10.X.X.200
XYZPCEUS02	10.X.X.201

XYZALKYS01	10.X.X.148
XYZCCRFW01A	10.X.X.184
XYZCCRFW02A	10.X.X.186

XYZDRBKUP	10.X.X.108
XYZPCEDC00	10.X.X.102
XYZPCEDC01	10.X.X.103
XYZPCNBKUP	10.X.X.107

XYZPCENM01	10.X.X.136

XYZPCEADMIN01	10.X.X.212
XYZPCEVXYZDMIN01	10.X.X.213

XYZAMC	10.X.X.16
XYZOPC10	10.X.X.20
XYZOPC20	10.X.X.21
XYZOPC30	10.X.X.22
OPCSRV1	10.X.X.9
OPCSRV2	10.X.X.10
OPCSRV4	10.X.X.12
OPCSRV6	10.X.X.14
OPCSRV7	10.X.X.15

XYZPCEDVMST01	10.X.X.204
XYZPCEDVMST02	10.X.X.205
XYZPCEDVMST03	10.X.X.206
XYZPCEDVMSVR01	10.X.X.200
XYZPCEDVMSVR02	10.X.X.201

ENGLAP10	10.X.X.60	ENGLAP11	10.X.X.55
ENGLAP11	10.X.X.55	ENGLAP12	10.X.X.61
ENGLAP13	10.X.X.63	ENGLAP1	10.X.X.48
ENGLAP3	10.X.X.49	ENGLAP5	10.X.X.50
ENGLAP6	10.X.X.51	ENGLAP7	10.X.X.53
ENGLAP8	10.X.X.56	ENGLAP9	10.X.X.58
XYZPCEAM01	10.X.X.19	XYZPCEAPC01	10.X.X.11
XYZPCEAPC02	10.X.X.12	XYZPCEAPC04	10.X.X.13
XYZPCEOPC01	10.X.X.7	XYZPCEOPC02	10.X.X.8
XYZPCEOPC03	10.X.X.9	XYZPCEOPC04	10.X.X.10
XYZPCETM01A	10.X.X.14	XYZPCETM01B	10.X.X.15
XYZPCETMWS01	10.X.X.18	VXPENGLAP7	10.X.X.54
ENGLAP5	10.X.X.50	ENGLAP6	10.X.X.51

ALKYGCCON01	10.X.X.5

ENTISRV01A	10.X.X.11
ENTISRV01B	10.X.X.12

FGACON02	10.X.X.45
USER-29F885DAD0	10.X.X.35

PSACON01	10.X.X.42

MITCON01	10.X.X.67
MITCON02	10.X.X.69

BOILER_HMI_1	10.X.X.66
BOILER_HMI_1	10.X.X.65
BOILER_HMI_2	10.X.X.68
BOILER_HMI_2	10.X.X.67

ALKYCEMCON01	10.X.X.121

COMBOCON1	10.X.X.149

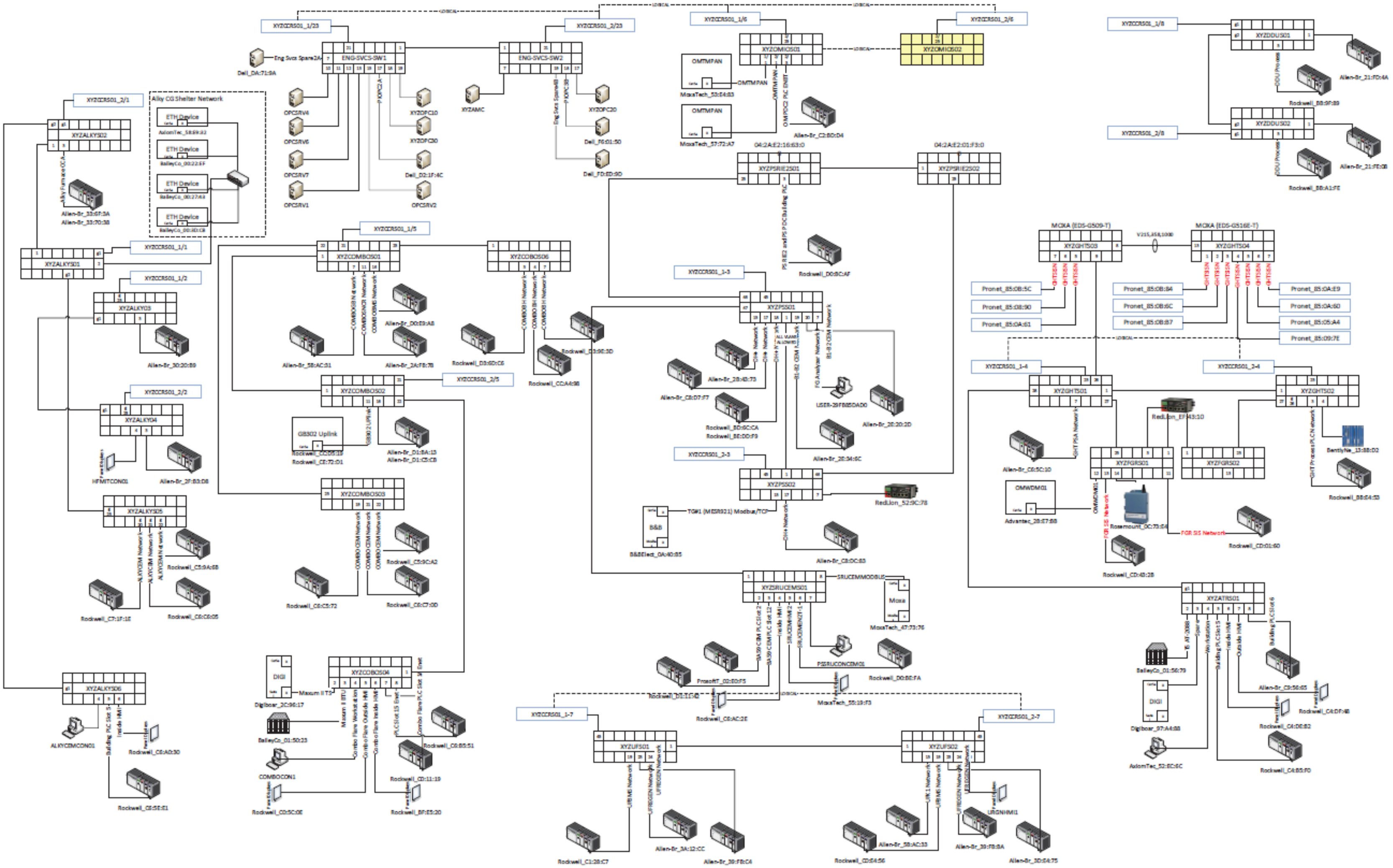
URGNHMI1	10.X.X.167
URGNHMI2	10.X.X.169

PSRUCONCEM01	10.X.X.233

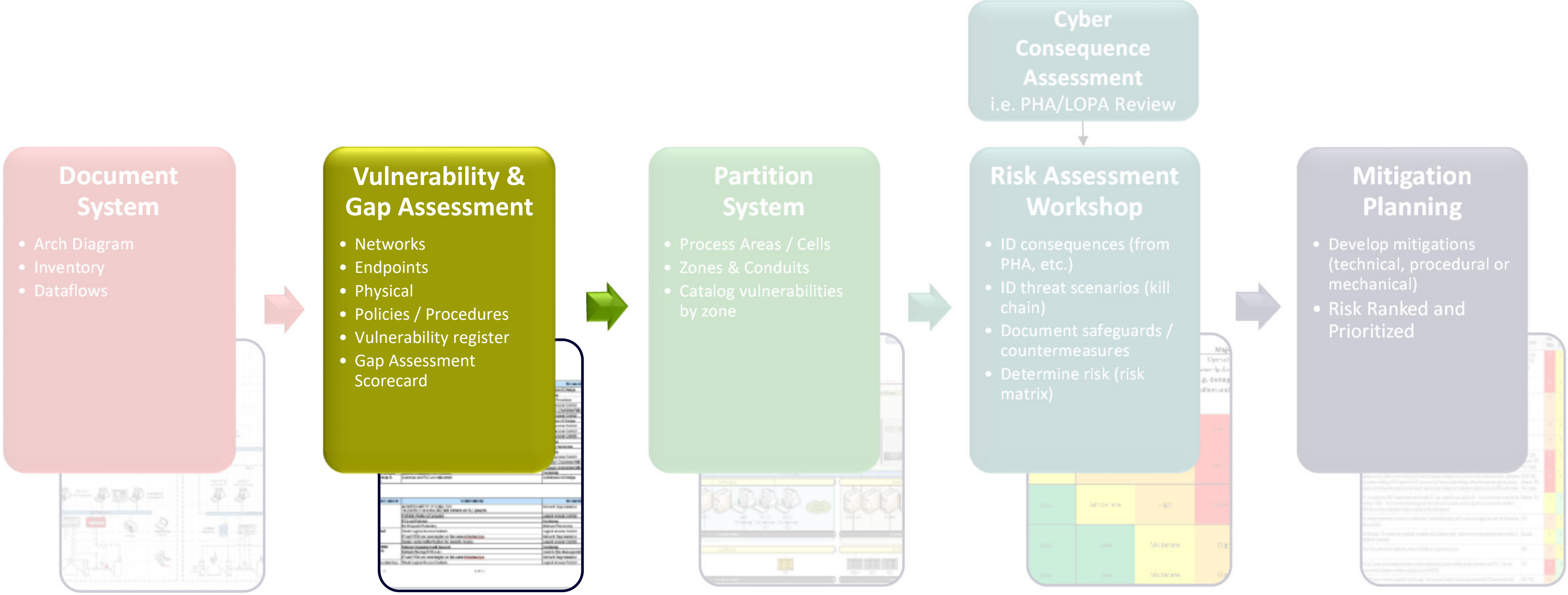
LEGEND

HOST	SIW Collected
HOST	From Monitoring Tool
HOST	From Site Asset Inventory
HOST	From PCAP
HOST	From Config File
SWITCH	MGMT IP of Switch

Example “As-Found” Physical Network Diagram



The CyberPHA Process



Cyber Consequence Assessment
i.e. PHA/LOPA Review

Document System
- Arch Diagram
- Inventory
- Dataflows

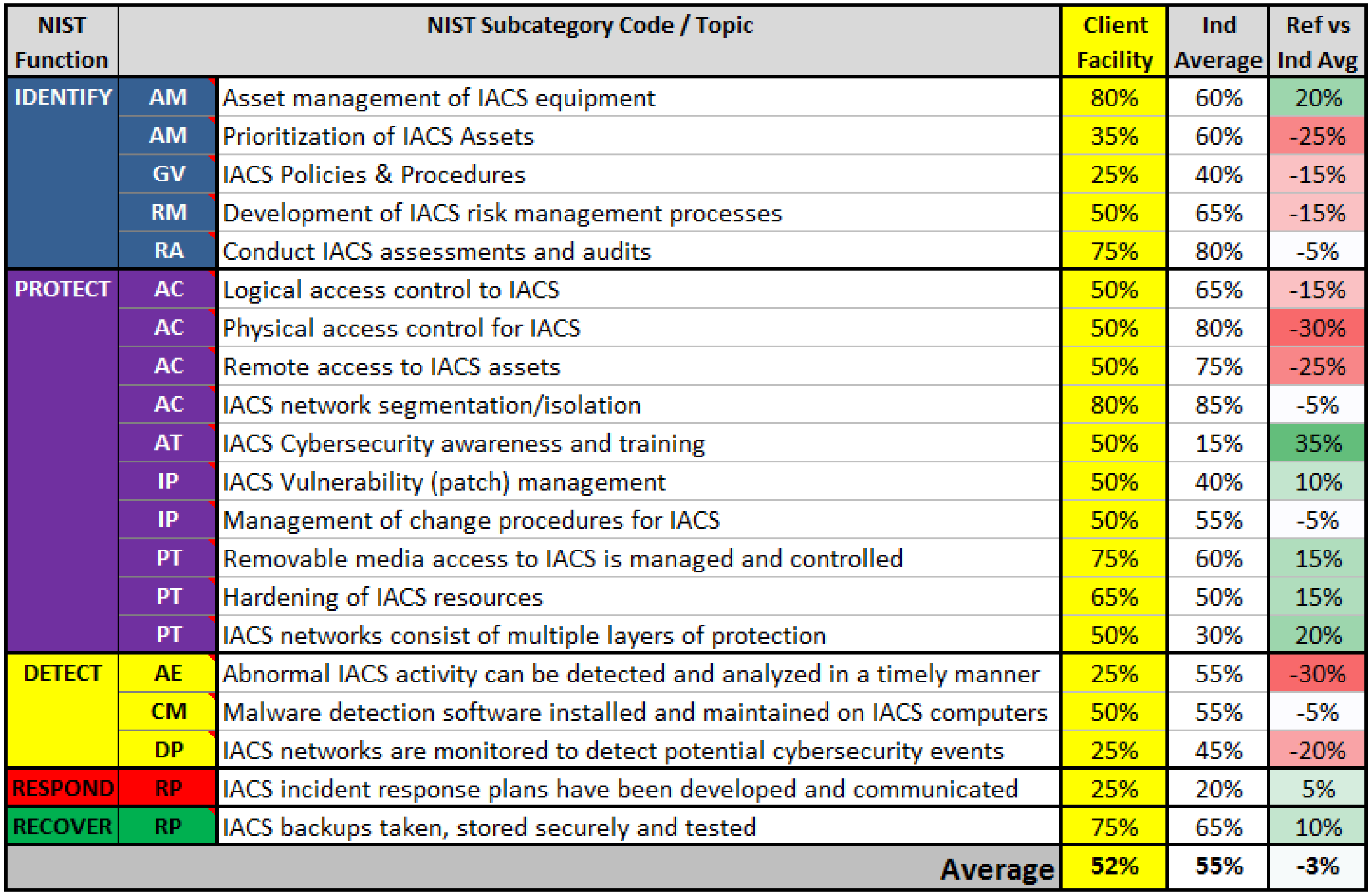
Vulnerability & Gap Assessment
- Networks
- Endpoints
- Physical
- Policies / Procedures
- Vulnerability register
- Gap Assessment Scorecard

Partition System
- Process Areas / Cells
- Zones & Conduits
- Catalog vulnerabilities by zone

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

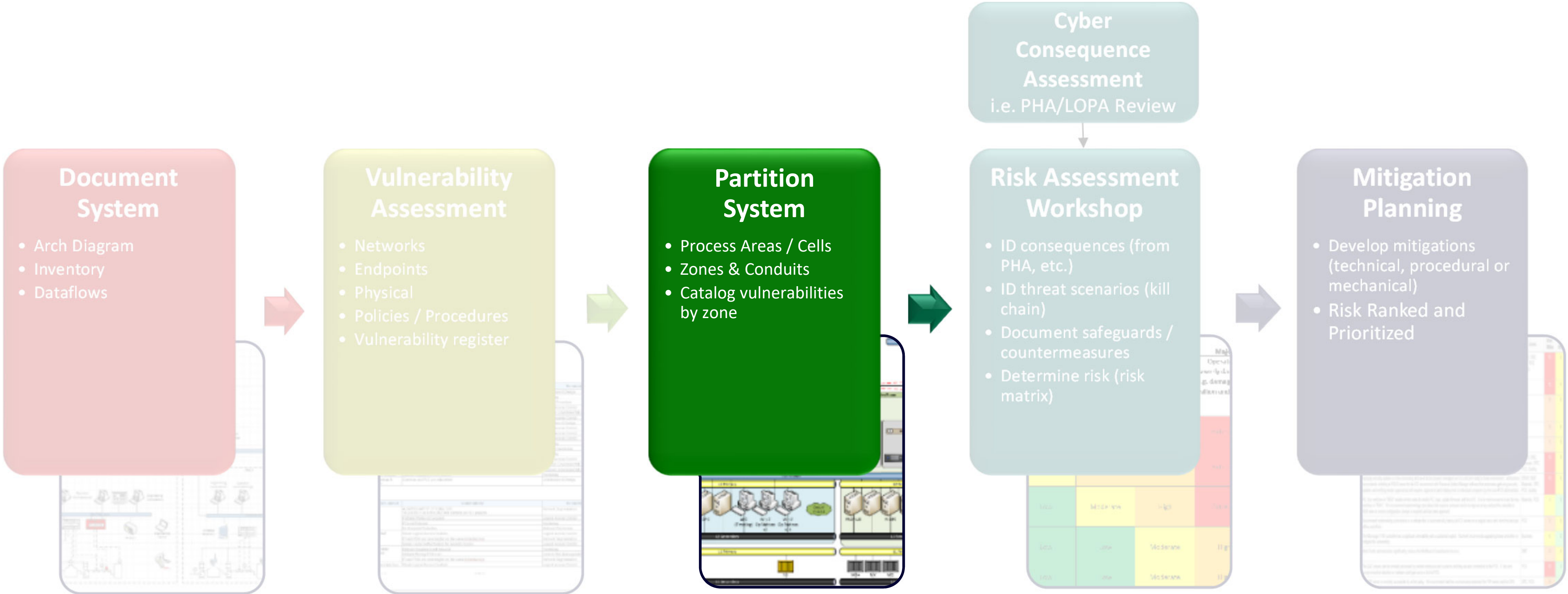
Mitigation Planning
- Develop mitigations (technical, procedural or mechanical)
- Risk Ranked and Prioritized

Peer Group Rankings



NIST Function	NIST Subcategory Code / Topic		Client Facility	Ind Average	Ref vs Ind Avg
IDENTIFY	AM	Asset management of IACS equipment	80%	60%	20%
	AM	Prioritization of IACS Assets	35%	60%	-25%
	GV	IACS Policies & Procedures	25%	40%	-15%
	RM	Development of IACS risk management processes	50%	65%	-15%
	RA	Conduct IACS assessments and audits	75%	80%	-5%
PROTECT	AC	Logical access control to IACS	50%	65%	-15%
	AC	Physical access control for IACS	50%	80%	-30%
	AC	Remote access to IACS assets	50%	75%	-25%
	AC	IACS network segmentation/isolation	80%	85%	-5%
	AT	IACS Cybersecurity awareness and training	50%	15%	35%
	IP	IACS Vulnerability (patch) management	50%	40%	10%
	IP	Management of change procedures for IACS	50%	55%	-5%
	PT	Removable media access to IACS is managed and controlled	75%	60%	15%
	PT	Hardening of IACS resources	65%	50%	15%
	PT	IACS networks consist of multiple layers of protection	50%	30%	20%
DETECT	AE	Abnormal IACS activity can be detected and analyzed in a timely manner	25%	55%	-30%
	CM	Malware detection software installed and maintained on IACS computers	50%	55%	-5%
	DP	IACS networks are monitored to detect potential cybersecurity events	25%	45%	-20%
RESPOND	RP	IACS incident response plans have been developed and communicated	25%	20%	5%
RECOVER	RP	IACS backups taken, stored securely and tested	75%	65%	10%
		Average	**52%**	**55%**	**-3%**

The CyberPHA Process



Cyber Consequence Assessment
i.e. PHA/LOPA Review

Document System
- Arch Diagram
- Inventory
- Dataflows

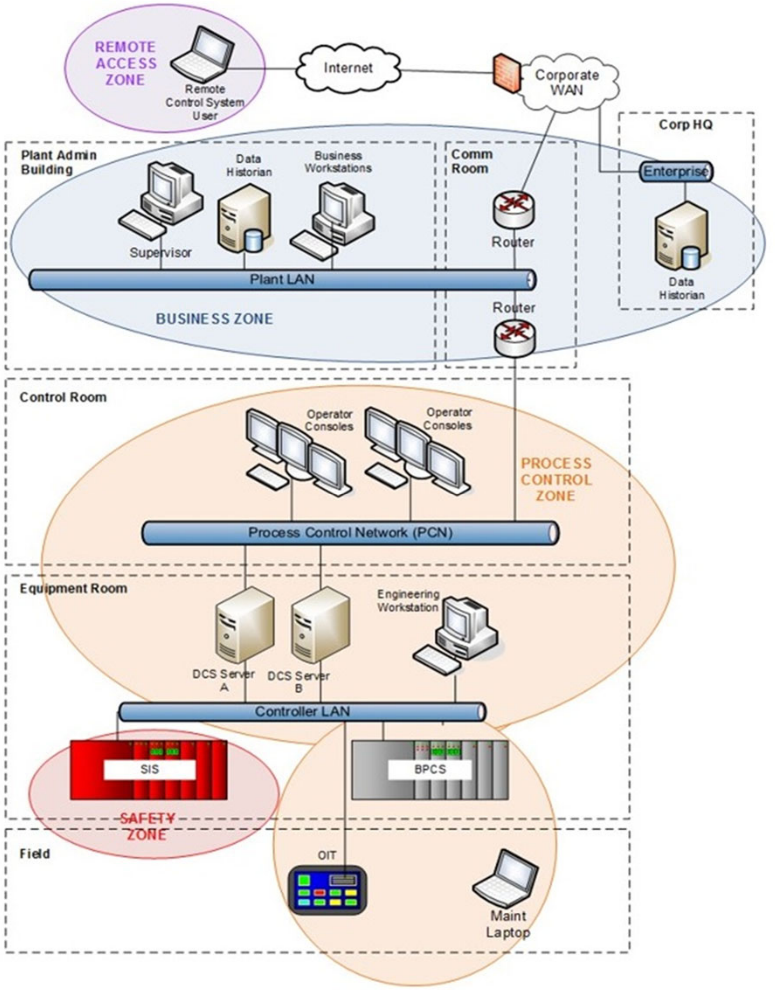
Vulnerability Assessment
- Networks
- Endpoints
- Physical
- Policies / Procedures
- Vulnerability register

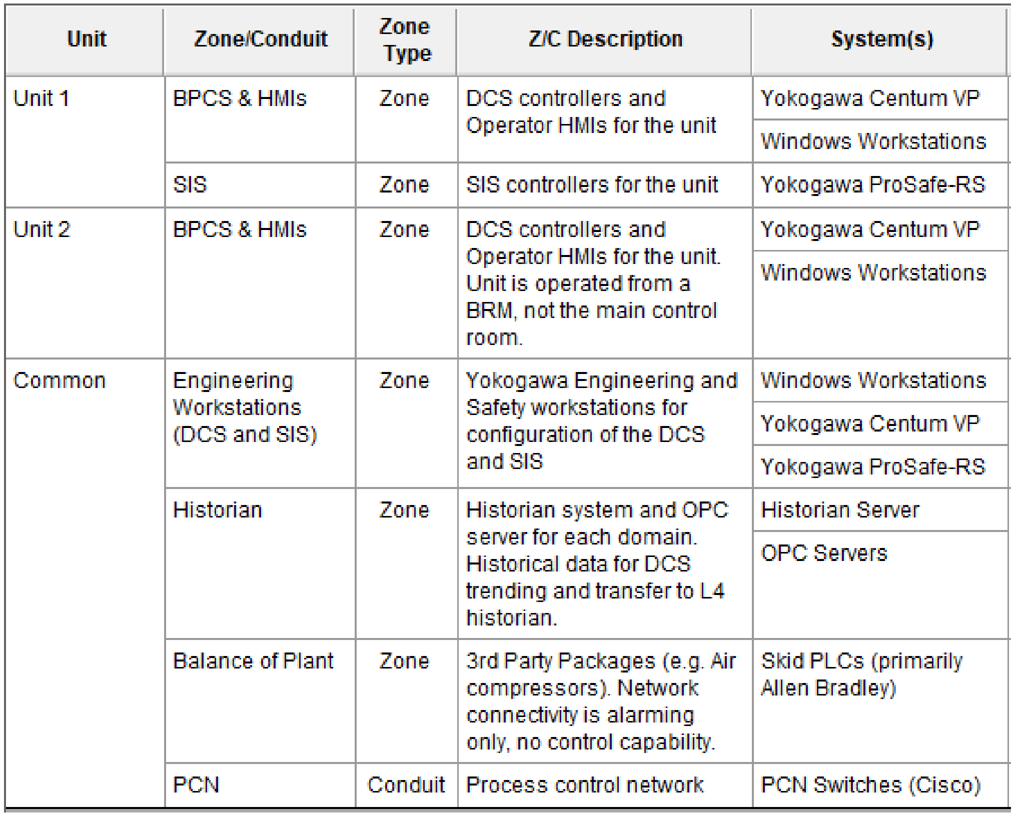
Partition System
- Process Areas / Cells
- Zones & Conduits
- Catalog vulnerabilities by zone

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

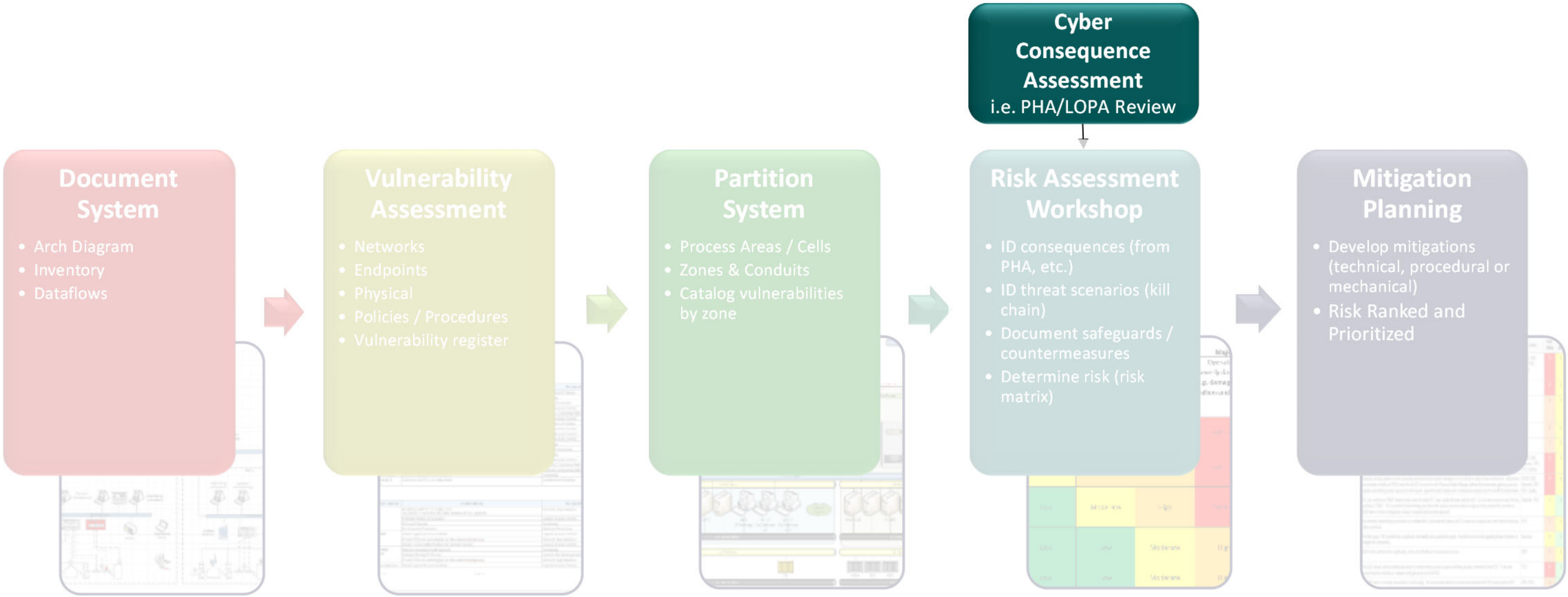
Example Zones/Conduits





Unit	Zone/Conduit	Zone Type	Z/C Description	System(s)
Unit 1	BPCS & HMIs	Zone	DCS controllers and Operator HMIs for the unit	Yokogawa Centum VP Windows Workstations
	SIS	Zone	SIS controllers for the unit	Yokogawa ProSafe-RS
Unit 2	BPCS & HMIs	Zone	DCS controllers and Operator HMIs for the unit. Unit is operated from a BRM, not the main control room.	Yokogawa Centum VP Windows Workstations
Common	Engineering Workstations (DCS and SIS)	Zone	Yokogawa Engineering and Safety workstations for configuration of the DCS and SIS	Windows Workstations Yokogawa Centum VP Yokogawa ProSafe-RS
	Historian	Zone	Historian system and OPC server for each domain. Historical data for DCS trending and transfer to L4 historian.	Historian Server OPC Servers
	Balance of Plant	Zone	3rd Party Packages (e.g. Air compressors). Network connectivity is alarming only, no control capability.	Skid PLCs (primarily Allen Bradley)
	PCN	Conduit	Process control network	PCN Switches (Cisco)

The CyberPHA Process



Cyber Consequence Assessment
i.e. PHA/LOPA Review

Document System
- Arch Diagram
- Inventory
- Dataflows

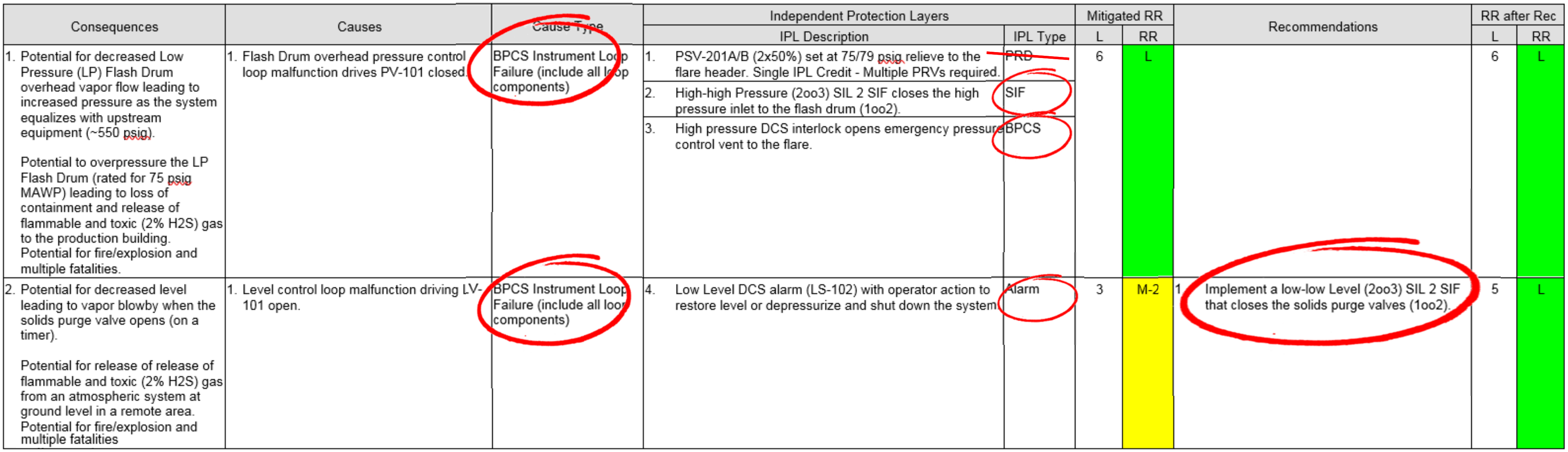
Vulnerability Assessment
- Networks
- Endpoints
- Physical
- Policies / Procedures
- Vulnerability register

Partition System
- Process Areas / Cells
- Zones & Conduits
- Catalog vulnerabilities by zone

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

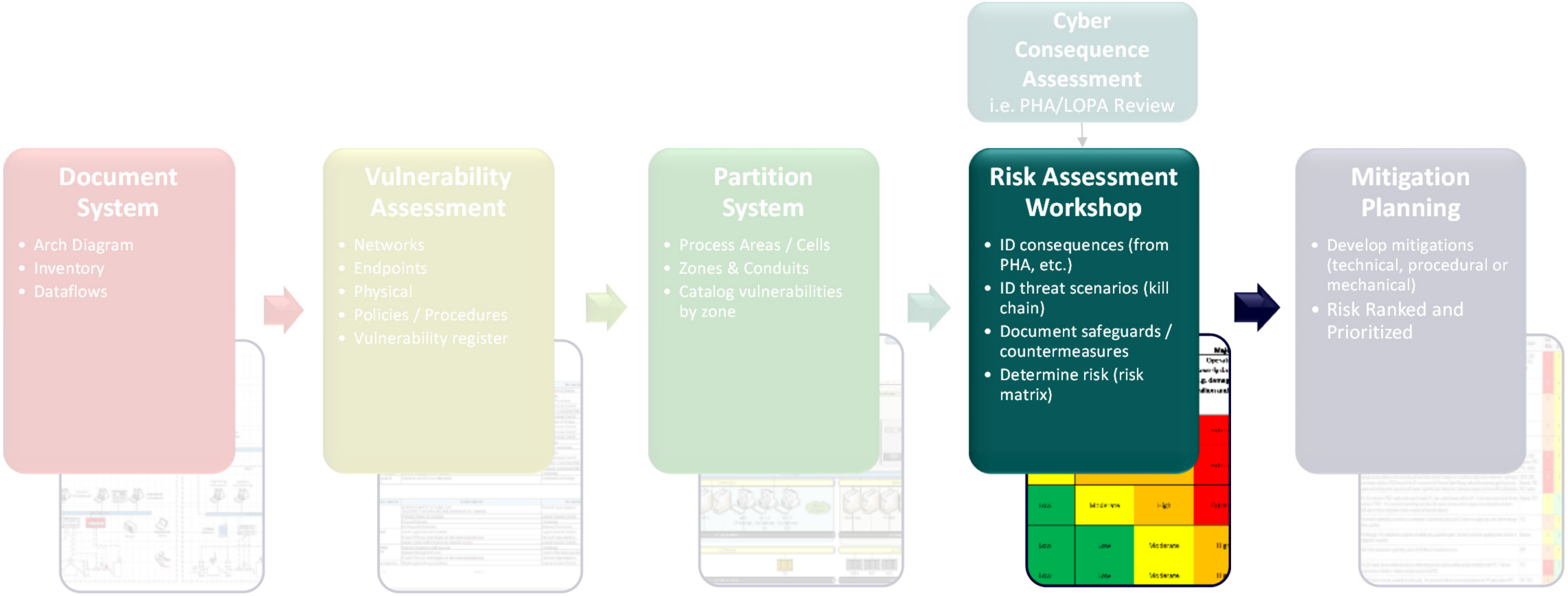
Mitigation Planning
- Develop mitigations (technical, procedural or mechanical)
- Risk Ranked and Prioritized

Cyber Consequence Assessment



Consequences	Causes	Cause Type	Independent Protection Layers		Mitigated RR		Recommendations	RR after Rec	
			IPL Description	IPL Type	L	RR		L	RR
1. Potential for decreased Low Pressure (LP) Flash Drum overhead vapor flow leading to increased pressure as the system equalizes with upstream equipment (~550 psig). Potential to overpressure the LP Flash Drum (rated for 75 psig MAWP) leading to loss of containment and release of flammable and toxic (2% H2S) gas to the production building. Potential for fire/explosion and multiple fatalities.	1. Flash Drum overhead pressure control loop malfunction drives PV-101 closed.	BPCS Instrument Loop Failure (include all loop components)	1. PSV-201A/B (2x50%) set at 75/79 psig relieve to the flare header. Single IPL Credit - Multiple PRVs required.	~~PRD~~	6	L		6	L
			2. High-high Pressure (2oo3) SIL 2 SIF closes the high pressure inlet to the flash drum (1oo2).	SIF					
			3. High pressure DCS interlock opens emergency pressure control vent to the flare.	BPCS					
2. Potential for decreased level leading to vapor blowby when the solids purge valve opens (on a timer). Potential for release of release of flammable and toxic (2% H2S) gas from an atmospheric system at ground level in a remote area. Potential for fire/explosion and multiple fatalities	1. Level control loop malfunction driving LV-101 open.	BPCS Instrument Loop Failure (include all loop components)	4. Low Level DCS alarm (LS-102) with operator action to restore level or depressurize and shut down the system	Alarm	3	M-2	1 Implement a low-low Level (2oo3) SIL 2 SIF that closes the solids purge valves (1oo2).	5	L

The CyberPHA Process



Cyber Consequence Assessment
i.e. PHA/LOPA Review

Document System

- Arch Diagram
- Inventory
- Dataflows

Vulnerability Assessment

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

Partition System

- Process Areas / Cells
- Zones & Conduits
- Catalog vulnerabilities by zone

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

The CyberPHA Team

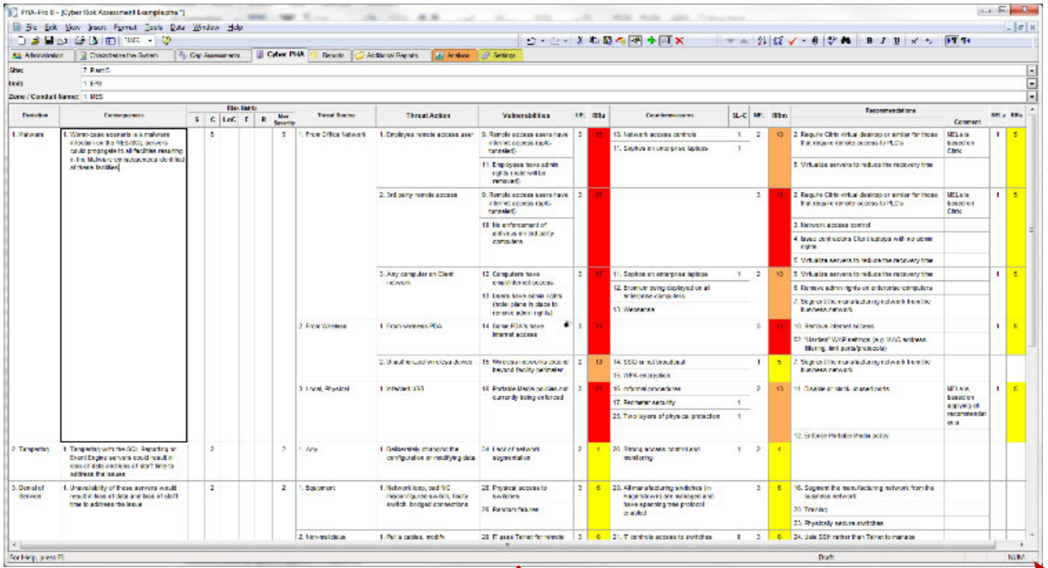
Collaborative Workshop Team

- Cybersecurity/Networking SME
- Process Safety/Controls SME
- Automation/Controls (Site)
- IT Applications (Site)

- Networking (Site)
- Information Security (Site)
- Process Safety (Site)
- Experienced Operator(Site)

CyberPHA Workshop Tools

Cyber PHA Worksheet



1. Malware

1. Worst-case scenario is a malware infection on the MES-SQL servers could propagate to all facilities resulting in the Malware consequences identified at those facilities

1. From Office Network

1. Employee remote access user

2. 3rd party remote access

9. Remote access users have internet access (split-tunneled)

11. Employees have admin rights (note will be removed)

10. No enforcement of antivirus on 3rd party computers

10. Network access controls

11. Sophos on enterprise laptops

2. Require Citrix virtual desktop or similar for those that require remote access to PLC's

5. Virtualize servers to reduce the recovery time

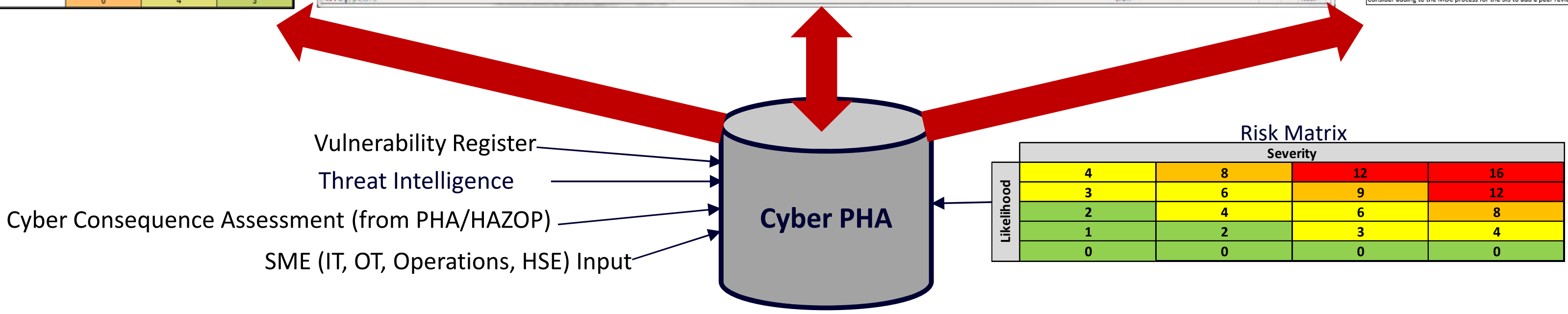
3. Network access control

Risk Register

Recommendation	Sites Used	Max RRu	Max RRm	Max RRa	Value Score
Consider option to increase the security of the wireless: Limit HTTP(S) sessions (timeout) Enable HTTPS Disable HTTP Disable CDP (Cisco discovery protocol) Restrict administrator access to only those required Enable time sync (NTP) Enable syslog	Baton Rouge, LA	A	A	D	14
Lock the ditch 5 pH and gyp stack wireless access point ports to prevent unauthorized access.	Baton Rouge, LA	A	A	D	14
Consider Escorted Access	Mooretown, ON	A	A	D	14
Follow up with LOPA team and ensure action on recommendation 65 from the LOPA report	Mooretown, ON	A	A	D	14
Consider implementing setpoint restraints on critical loops	Mooretown, ON	A	A	D	9
Consider options to reduce the risk associated with the ability to pivot to DeltaV (third NIC) across ControlNet. Options to consider: Firewall VLAN Segmentation VRF (virtual routing and forwarding)	Baton Rouge, LA	A	A	D	6
Investigate options for monitoring and alerting including: Security Information and Event Monitoring and Alerting IDS (Intrusion Detection)	Baton Rouge, LA	A	A	D	4
EWS should be logged off when not in use	Macon, GA	B	B	D	14
·Consider leaving PLC key switch in "Run" position for those controllers which do not require logic changes; this ensures that someone local is aware of PLC changes.	Greenville, NC	B	B	D	14
Consider Securing Portable Media	Greenville, NC, Mooretown, ON	B	B	D	14
Consider implementing a process where portable media is scanned prior to use	Greenville, NC	B	B	D	14
Consider the following options to increase the security of the Lab/Test Beds: VLAN Isolation	Baton Rouge, LA	B	B	D	14
Consider keeping Controllers in Run and Removing the Key	Sandusky, OH	A	B	D	14
Consider creating a subset of authorized users with access to the softrware Estop button	Sandusky, OH	B	B	D	14
Consider logging out of the supervisor account on the console currently left logged in.	Mooretown, ON	B	B	D	14
Consider changing the priviledges of the supervisor account to limit access to critical alarms and setpoints	Mooretown, ON	B	B	D	14
Consider securing User Accounts with Least Privilege	Mooretown, ON	B	B	D	14
Consider Securing Portable Media (disable physically or logically)	Mooretown, ON	B	B	D	14
Consider alarms for bypassed inputs in the SRS.	Mooretown, ON	A	B	D	14
Consider adding to the MOC process for the SIS a step to require offline testing of new logic before downloading	Mooretown, ON	B	B	D	14
Consider adding to the MOC process for the SIS to add a peer review step before	Mooretown, ON	B	B	D	14

Risk Profile

Site	Unit	Zone	Unmitigated Risk (no countermeasures)	Mitigated Risk (existing countermeasures)	Adjusted Risk (proposed countermeasures)
1. Anywhere	1. Remote	1. Employee Remote Access	8	6	3
2. Corporate HQ	1. Corporate	1. Enterprise	7	5	4
3. Terminal	1. Admin Building	1. Plant Business	5	4	3
	2. Truck Loading	1. Process Control	8	6	5
		3. Safety	10	6	4
		5. Wireless	6	4	3
	3. Tank Farm	1. Process Control	9	7	4
		5. Wireless	6	4	3
3. Pumping Station	1. Admin Building	1. Plant Business	5	4	3
	2. Pump House	1. Process Control	8	5	4
		3. Safety	10	6	4
	3. Tank Farm	1. Process Control	8	6	5
		5. Wireless	6	4	3



Vulnerability Register

Threat Intelligence

Cyber Consequence Assessment (from PHA/HAZOP)

SME (IT, OT, Operations, HSE) Input

Cyber PHA

Risk Matrix

Likelihood	Severity			
	4	8	12	16
	3	6	9	12
	2	4	6	8
	1	2	3	4
	0	0	0	0

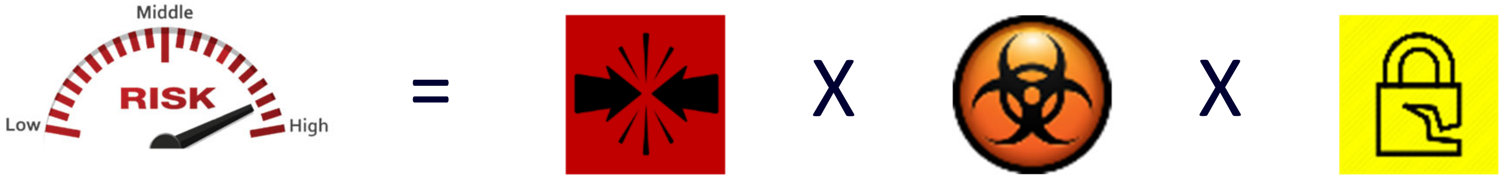
Risk and Security Risk

Risk - "(exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility" – Oxford English Dictionary, 3rd ed.

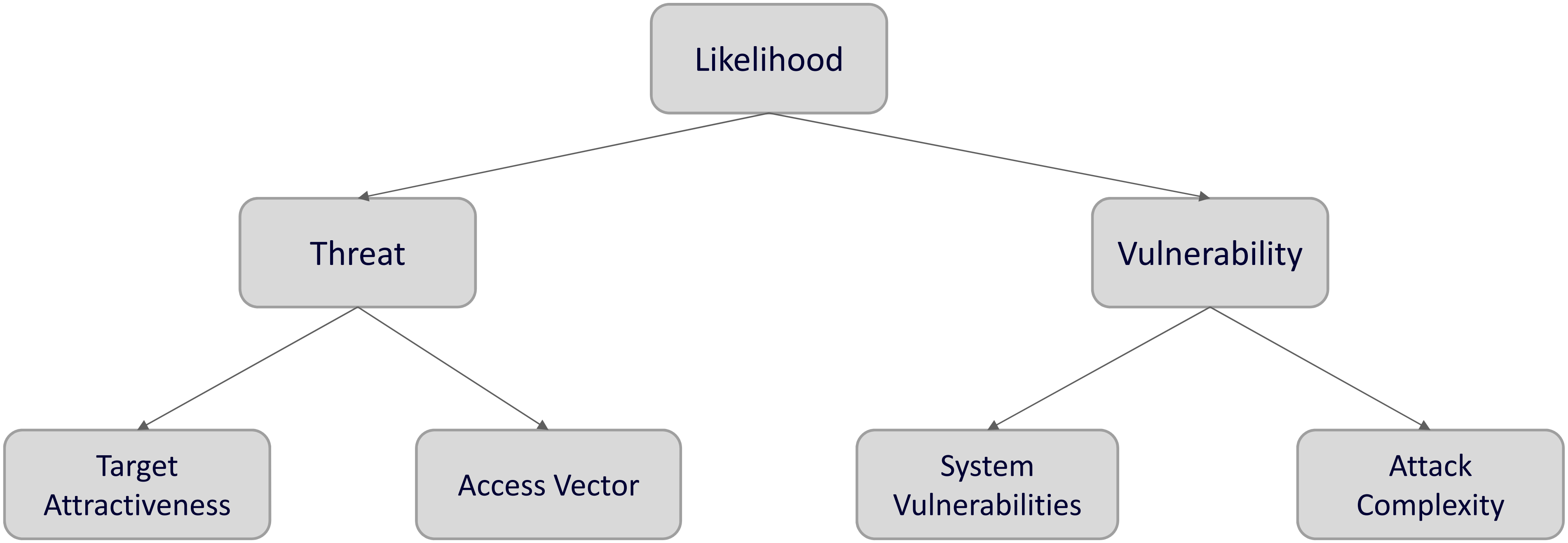
Risk = Impact x Likelihood

"***[Security] Risk*** is a function of the likelihood of a given *threat-source* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization." – NIST SP800-30

Security Risk = Impact x (Threats x Vulnerabilities)



Cybersecurity Likelihood



Likelihood

Threat

Vulnerability

Target Attractiveness

Access Vector

System Vulnerabilities

Attack Complexity

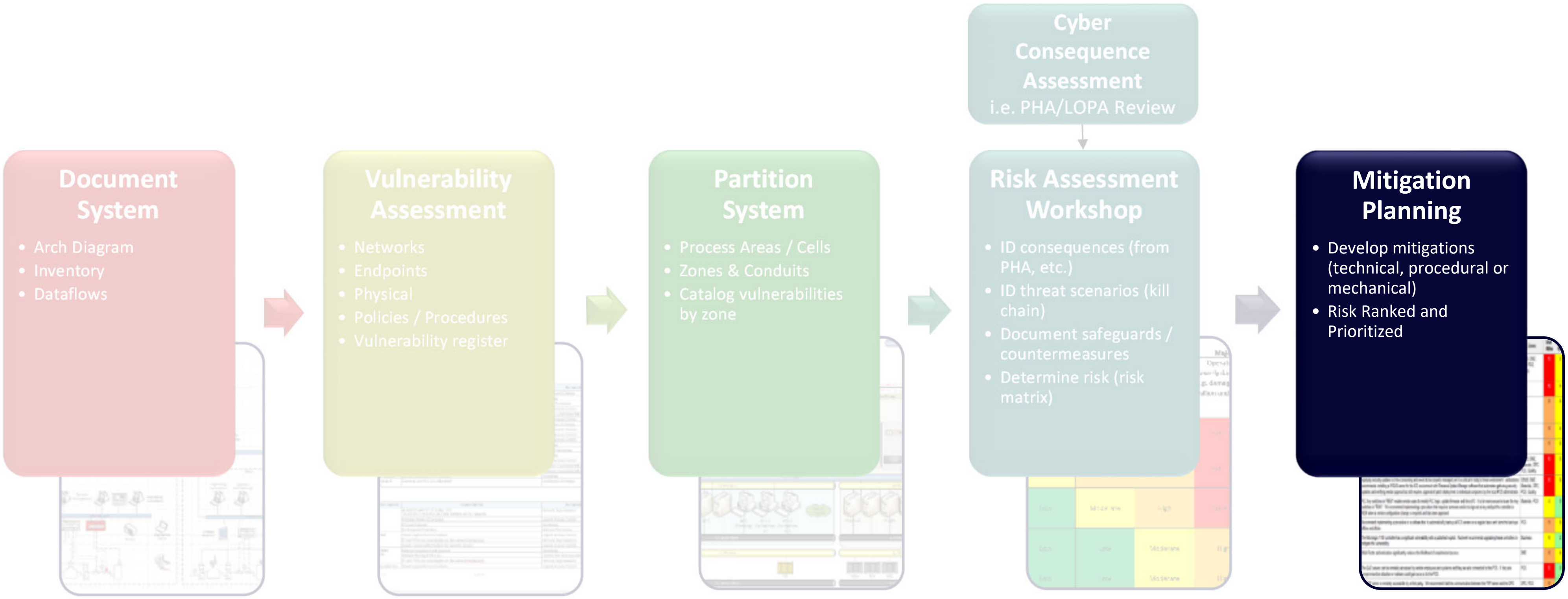
The value of a facility or industry as a target to an adversary

What type of access is required to attack the system. e.g. local, adjacent network, remote.

The number, types, and severity of vulnerabilities present in a system

How easy or difficult it is to exploit the discovered vulnerabilities

The CyberPHA Process



Document System

- Arch Diagram
- Inventory
- Dataflows

Vulnerability Assessment

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

Partition System

- Process Areas / Cells
- Zones & Conduits
- Catalog vulnerabilities by zone

Cyber Consequence Assessment

i.e. PHA/LOPA Review

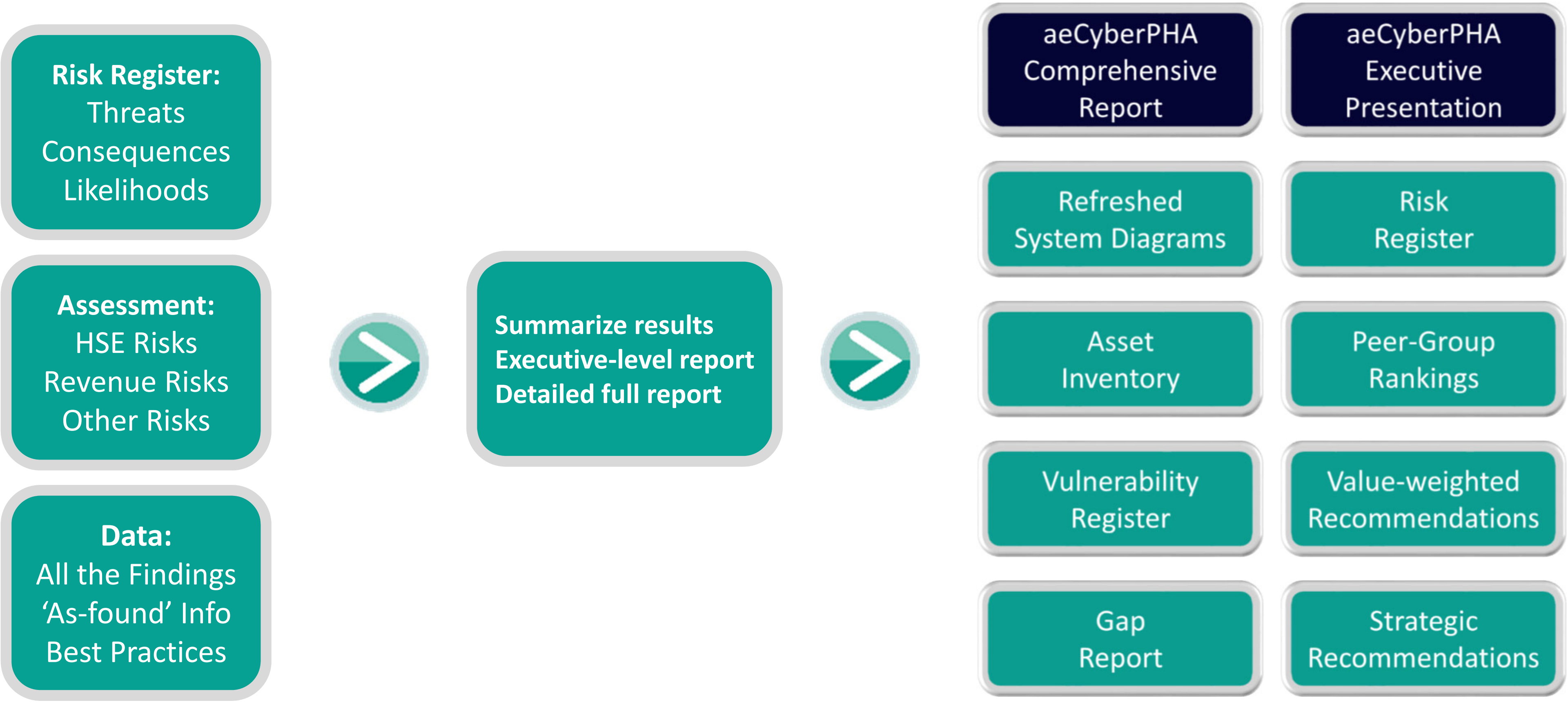
Risk Assessment Workshop

- 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

CyberPHA Reporting



Risk Register:
Threats
Consequences
Likelihoods

Assessment:
HSE Risks
Revenue Risks
Other Risks

Data:
All the Findings
'As-found' Info
Best Practices

Summarize results
Executive-level report
Detailed full report

aeCyberPHA Comprehensive Report

aeCyberPHA Executive Presentation

Refreshed System Diagrams

Risk Register

Asset Inventory

Peer-Group Rankings

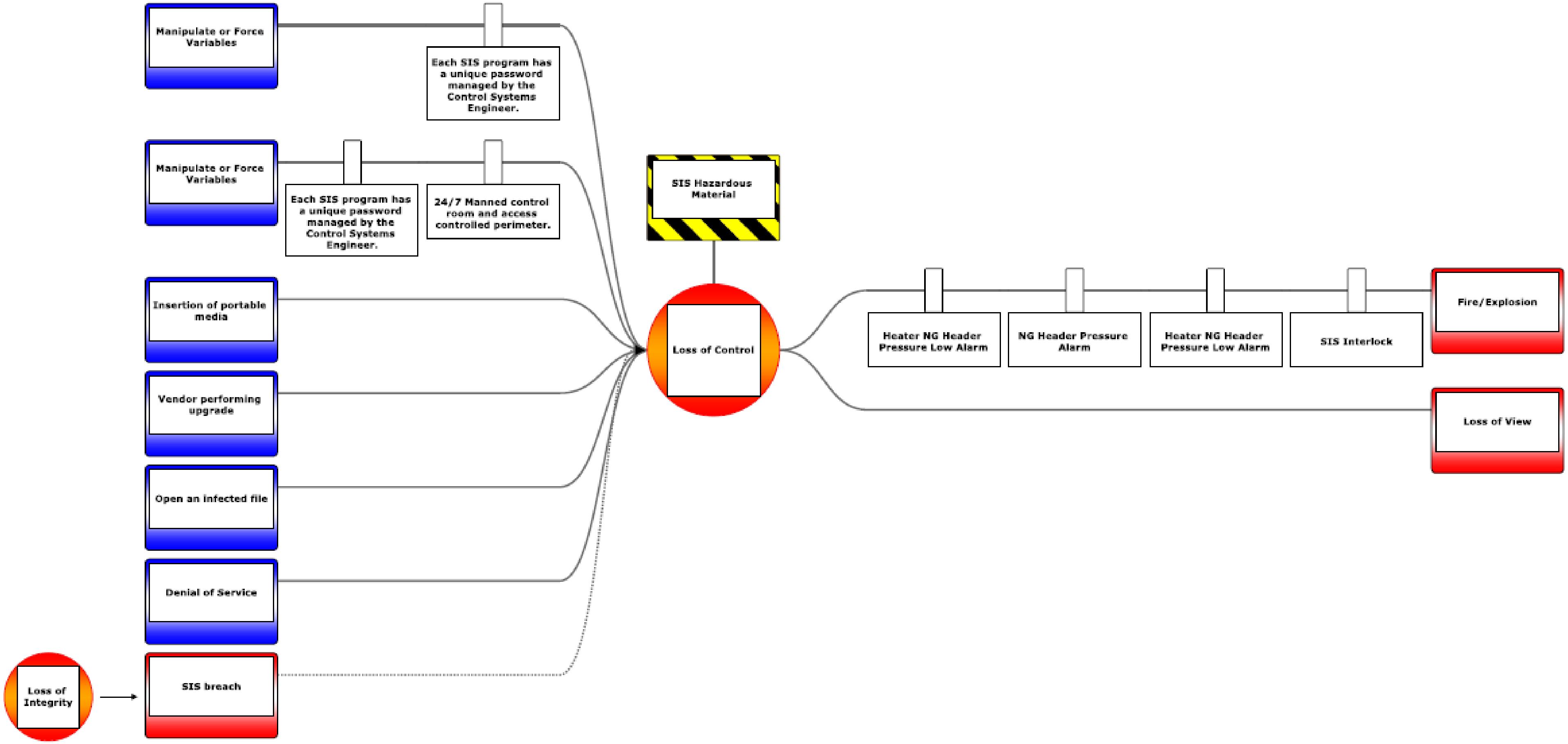
Vulnerability Register

Value-weighted Recommendations

Gap Report

Strategic Recommendations

Cybersecurity Bowties


Manipulate or Force Variables
Each SIS program has a unique password managed by the Control Systems Engineer.
Manipulate or Force Variables
Each SIS program has a unique password managed by the Control Systems Engineer.
24/7 Manned control room and access controlled perimeter.
Insertion of portable media
Vendor performing upgrade
Open an infected file
Denial of Service
Loss of Integrity
SIS breach
SIS Hazardous Material
Loss of Control
Heater NG Header Pressure Low Alarm
NG Header Pressure Alarm
Heater NG Header Pressure Low Alarm
SIS Interlock
Fire/Explosion
Loss of View

For More Information

www.aesolns.com

John Cusimano, CISSP, GICSP, CFSE
VP of Industrial Cybersecurity
John.Cusimano@aesolns.com

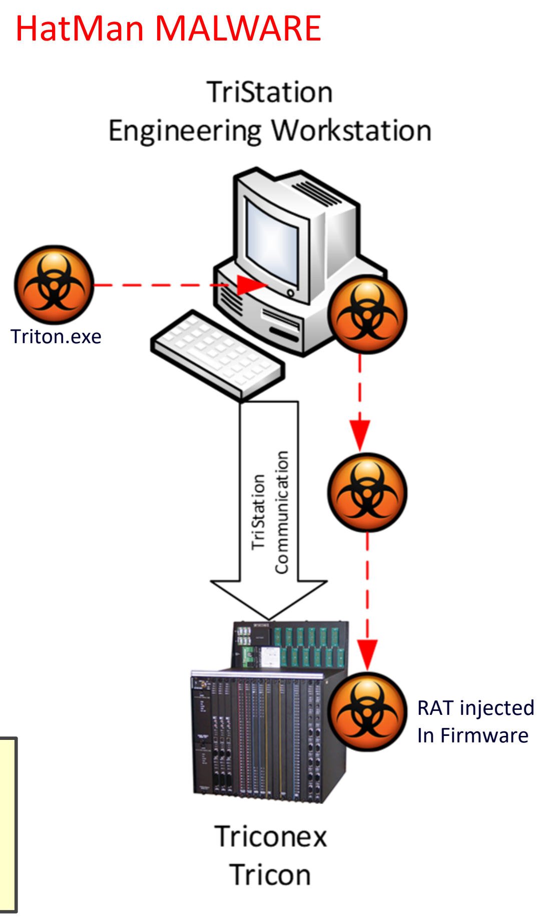
Jacob Morella, PE, GICSP, CFSE
IC Technical Project Manager
Jacob.Morella@aesolns.com

aE Solutions™

HatMan (aka Triton/TriSIS) Malware

- Sophisticated malware targeting Triconex SIS
- Detected in Nov 2017 in the Middle East
- First reported cyber attack on a safety instrumented system (SIS)
- Two-stage attack
  - Compromise TriStation engineering workstation
  - Place a Remote Access Trojan (RAT) on the SIS controller
- Discovered due to bug in the malware that caused the SIS to trip (failsafe)

Just because a SIS is SIL rated does not mean it is immune to cyber threats

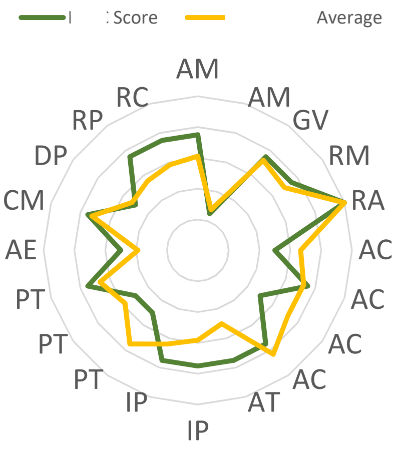


REFINERY #3

Critical Findings

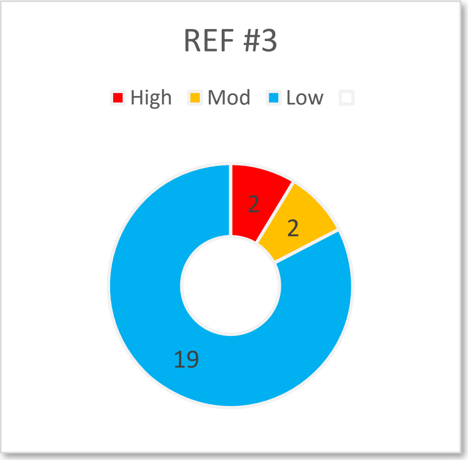
- Automatic file replication between business and PC through mapped drives
- Domain admin accts with elevated privileges on Honeywell servers
- AMS system enables remote modification of field devices from L3

Compliance



66%

Risk



High Risk Zones:

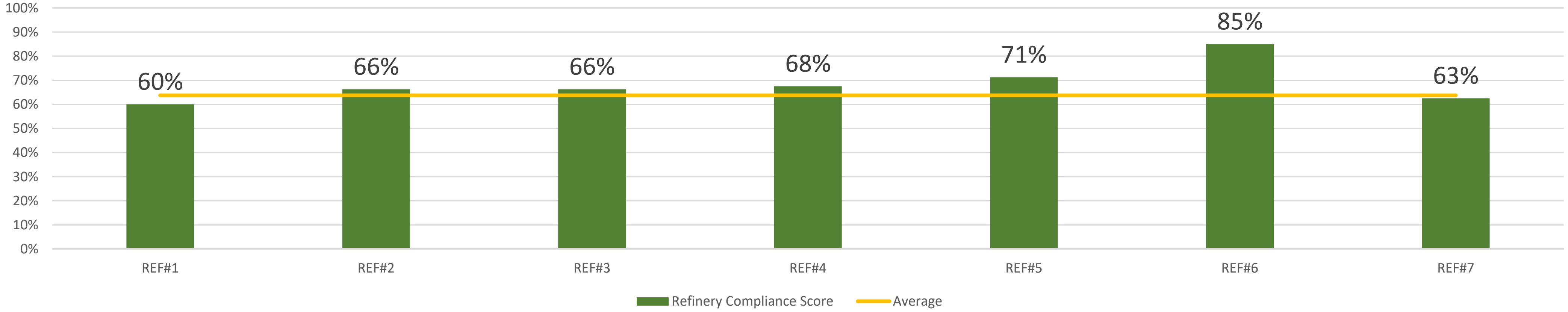
- DMZ36
- PCN

Mod Risk Zones:

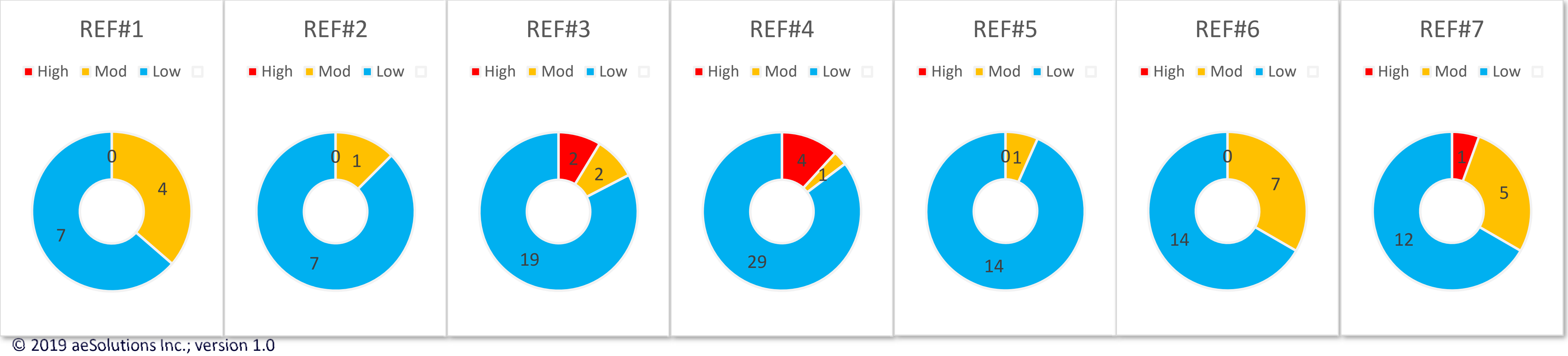
- AMS
- Domain Services

Summary of Compliance and Risk Assessments

COMPLIANCE GAP SCORES



RISK PROFILES


REF#1
High Mod Low
REF#2
High Mod Low
REF#3
High Mod Low
REF#4
High Mod Low
REF#5
High Mod Low
REF#6
High Mod Low
REF#7
High Mod Low