OT Vulnerability Management as a business enabler

Craig Morris

AISA

About me

- Director OT Cybersecurity – KPMG
- Ex-CISO (Middle East)
- Ex-Asset Owner

camorrisaus

Infosecmorc

AISA

PERTHISEC

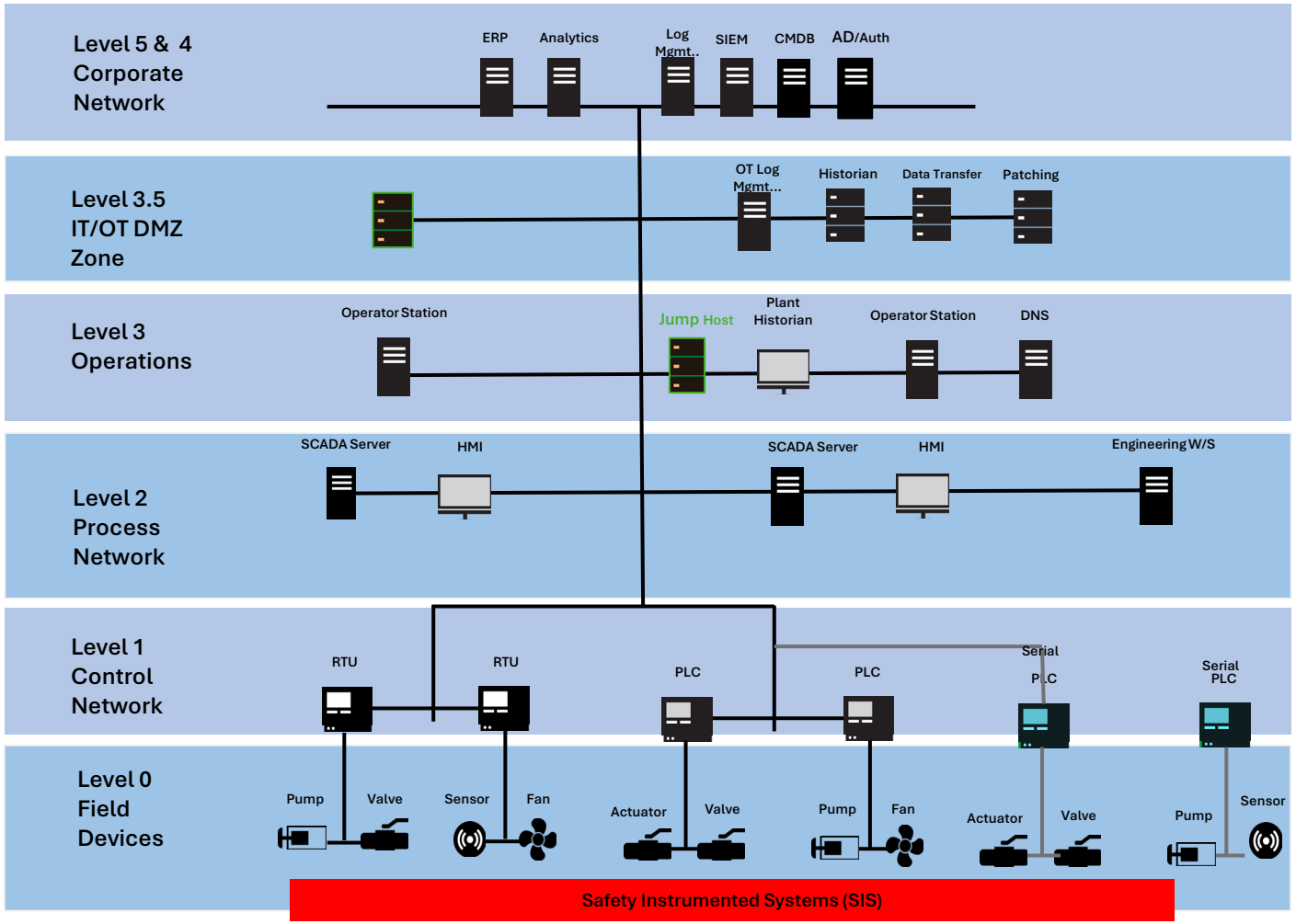
So what is the problem?

- Governance, ownership, responsibility
- Risk of downtime, Consequences
- Complexity, expensive
- Legacy systems & Obsolescence
- OT assets insecure by design
- Poor architecture and controls
- Resource capability/capacity
- Vendor/SI Contractual requirements
- Changing Threat Landscape

Purdue Reference Model

IT

OT



Microsoft, Cisco, Linux
Appliances (Linux-based)
AD, MS SQL etc, common web services, applications

Microsoft, Linux
AD, HMI's Historians (Pi, IP21 etc)
Cisco, RuggedCom, MOXA, Hirschman
SCADA/DCS Apps, SCADA Tools,
OT protocols (Proprietary, IP, Serial)

Physical hardware (PLC's etc) ,
Custom Realtime OS (WindRiver, VxWorks)
Firmware
Proprietary protocols

***NOTE**: Vendors and products are indicative only and do not represent an endorsement in any way.*

Global Vulnerability Statistics 2023/2024

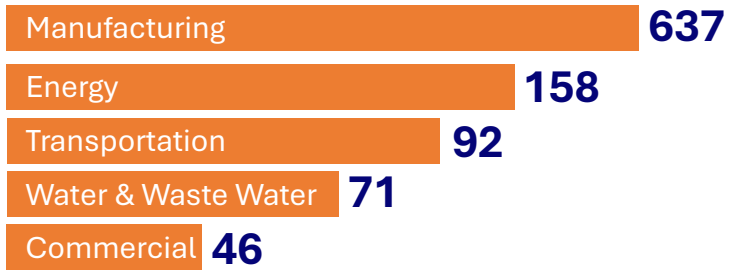
134
New advisories (CISA)

842
New vulnerabilities Disclosed

49
Impacted automation vendors

Top 5 Sectors

Impacted by disclosed vulnerabilities



73%
Advisories have **no known practical**, vendor remediation,

54%
Incidents exploited **known** vulnerabilities

80%
Vulnerabilities reside deep **within OT** networks (L2, L1)

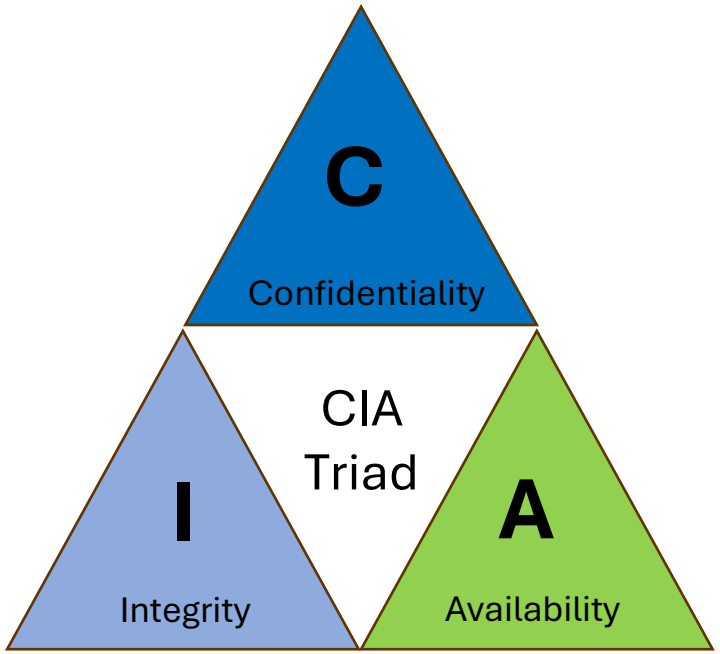
16%
Network **exploitable and Internet facing**

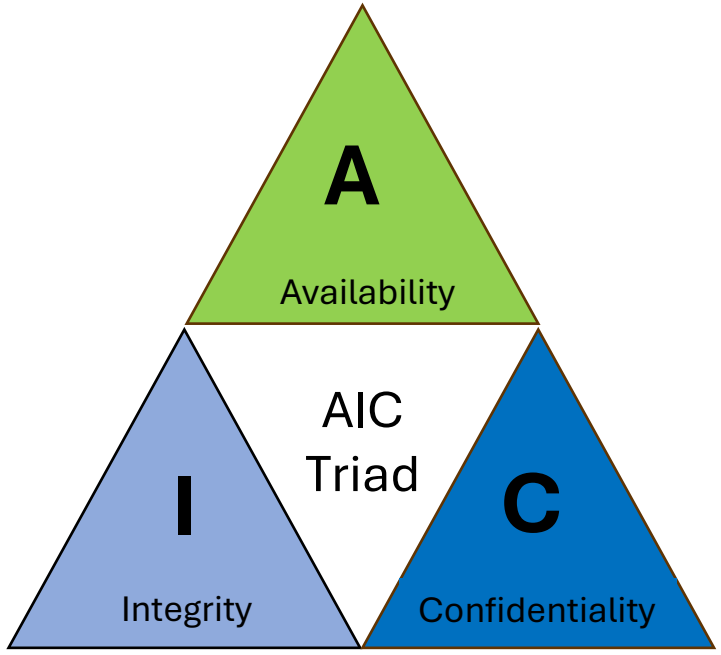
68%
Incidents – could be prevented through proper **architecture**

70%
OT attacks originated **from IT** environment

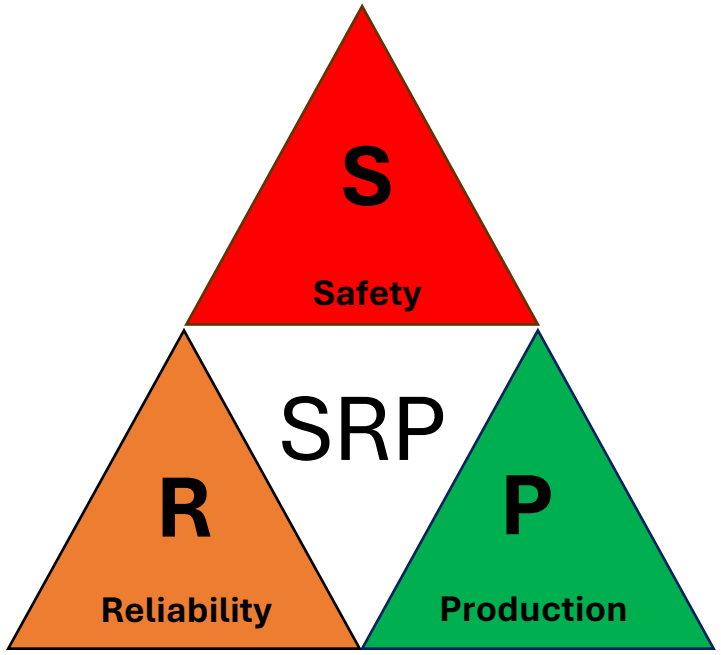
Sources : Nozomi OT/Iot Cybersecurity Trends and Insights 2024 H1
Dragos 2023 OT Cybersecurity Year in Review

What are we protecting in OT environments?





Getting warmer ...



- **Physics & Engineering**
- **Consequences**
- **Context**

Patching versus Vulnerability Management

Patching

- Tactical activity
- Point in time – known issues (CVSS etc, Vendors)
- Event driven (New vulnerability, patch is available?)
- Specific software updates for ***supported*** systems
- Subset of Vulnerability Management

V

Vulnerability Management

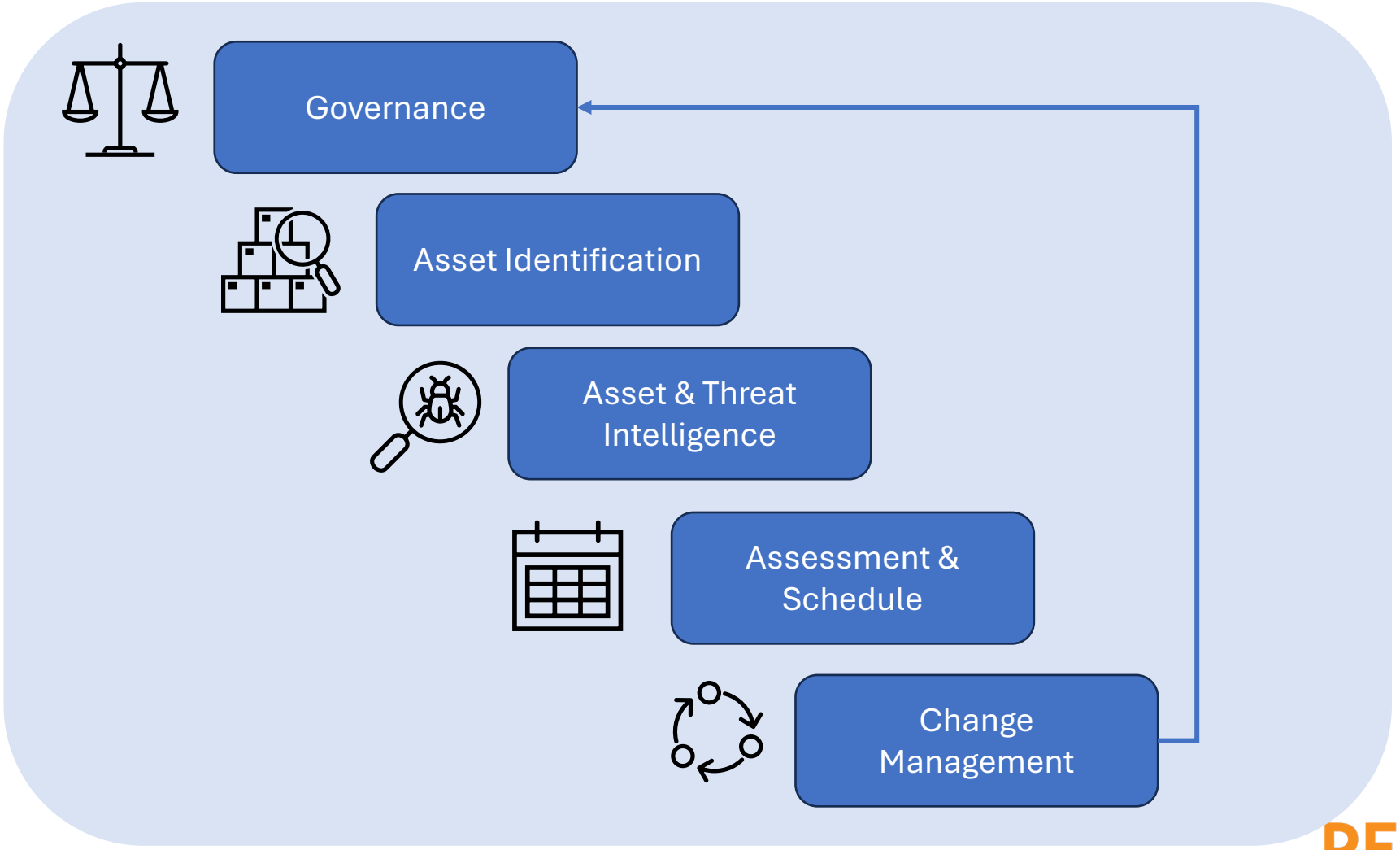
- Strategic approach
- Continuous, proactive identification, assessment, remediation of vulnerabilities, misconfigurations
- Risk driven (in theory) – business, operational, safety requirements
- All systems even ***unsupported*** systems
- Remediation may include patching, configuration changes, monitoring

OT Vulnerability Management - Business Enablement

Data

- Organisation Mission, Business Value
- Enterprise Asset Management *(SOCI)*
- Governance, Assurance, Reporting *(SOCI)*
- Business & Operational Resilience *(SOCI)*
- Crisis Management *(SOCI)*

Establishing an OT Vulnerability Management Program

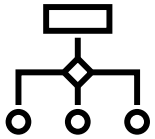


Governance – Essential to success

Who has ultimate responsibility and decision making for significant risks and vulnerabilities?

Key Stakeholders

- COO (or equiv.)
- CISO
- Chief Engineer
- OT Engineer(s)
- Cyber Engineers(s)



Structure

- SteerCo ☺
- Working Group ☺
- Re-org ☹

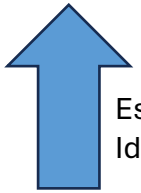
Charter

- Purpose & Mission
- Authority
- Schedule
- Roles & Resp.
- Escalation

Reporting

- Metrics
- Reporting cycle

Direction, decisions, budget



Escalation, Risk Identification, Reporting

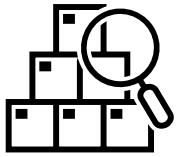
Local OT Engineers, Site Support, 3rd Party support, IT support

AISA

PERTHSEC

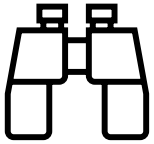
Asset Identification – What do we have

What do we have, where, and what condition is it in?



Identification

- Walk downs
- Manual entry
- Automated
- Diagrams
- Purchase Orders



Classify Assets

- Ownership
- Function
- Risk level (Assess)
- Criticality
- Impact (BIA)
- ** SOCI ??

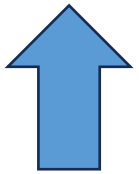
Asset Register

- Asset ID
- Versions
- Components – RAM, CPU, IP etc
- Dependencies
- Ownership
- Current state

Maintain

- Secure storage
- Regular reviews
- Updates

Known asset condition, Ownership, Criticality



BIA and Criticality changes
Ownership changes, Obsolescence plans

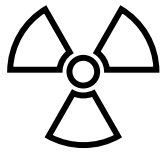
Asset Lifecyle, Obsolescence, Incident Response, Business Impact Analysis

Asset & Threat Intelligence – Are we vulnerable?

Where are our risks, how do we know we have risks, and how do we ensure we stay up to date with risks and changes in environment

Assess Risks

- High level assessment
- Baseline/current state of assets
- Prioritise Assets
- Additional controls?



Risk Info Sources

- Vulnerability Assessments
- Penetration tests
- Audit reports
- Threat Intel feeds
- CVSS, KEV, EPSS
- Mitre ATT&CK ICS
- News, Blogs
- External - ACSC etc

Visibility

Continuous :

- Asset Identification
- Vulnerability Identification
- Anomaly detection

When do we worry? CVSS v KEV v EPSS ?

CVE = Common Vulnerabilities and Exposures – ID assigned to a vulnerability

	Common Vulnerability Scoring System v4 (CVSS)	Known Exploited Vulnerabilities (KEV)	Exploit Prediction Scoring System v2 (EPSS)
Approach	Assigns score for severity based on multiple factors - **Calculated score.**	Known vulnerabilities (CVE), **actively exploited and clear remediation available**	Likelihood/Probability (0-1, 0 – 100%) that a vulnerability **will be** exploited within **30 days.** Data driven
Drawbacks	High CVSS scores ≠ High Risk	Not all active CVE's covered by KEV	Only covers vulnerabilities with a CVE ID, can produce false positives and negatives

Use in combination – none provide full coverage

Assessment Criteria – How do we decide?

Initial view - How do we know what to remediate and when? We cannot do everything so how do we prioritise?

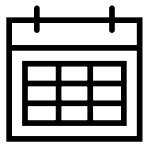
Exposure
- Is vulnerability applicable?
- Asset Criticality
- Internal or Internet Facing
- Current controls?

Safety Impact
- Vulnerability impact to Safety?
- Remediation impact to Safety?

Security Posture
- Current state?
- Will remediation make a difference?

Process Impact
- Asset role in process?
- Impact on process (Safety,Reliability, Production)?
- Cost to implement & test , revalidate ($, Time)

Technical Impact
- Remediation available?
- Alternate Remediation options?
- *CVSS, KEV, EPSS scores*



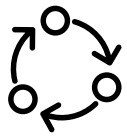
Schedule Decision

- **Now** – As soon as possible
- **Next** – Next available shutdown/outage
- **Never** – Do not apply. Has no impact on risk reduction *

* Asset owner may decide to patch based on maintenance, improvements etc (not cyber requirements)

Change Management - making safe changes

Ensuring the change is tested, performed and verified so there is no impact to the OT processes.

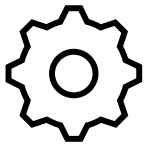


Plan Change

- Scheduling
- Safety requirements
- Vendors/3rd Parties
- Stakeholders
- Site resource availability
- CAB Engagement
- Management of Change (MOC)

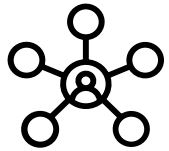
Testing

- Offline
  - Test Lab
  - Vendor Lab
- Online ☹
- Test remediation effectiveness
- Verification Plan
- Rollback Plan



Perform Change

- Staff available
- Stakeholders advised
- Systems backed up
- Implementation
- Update docs & diagrams!!

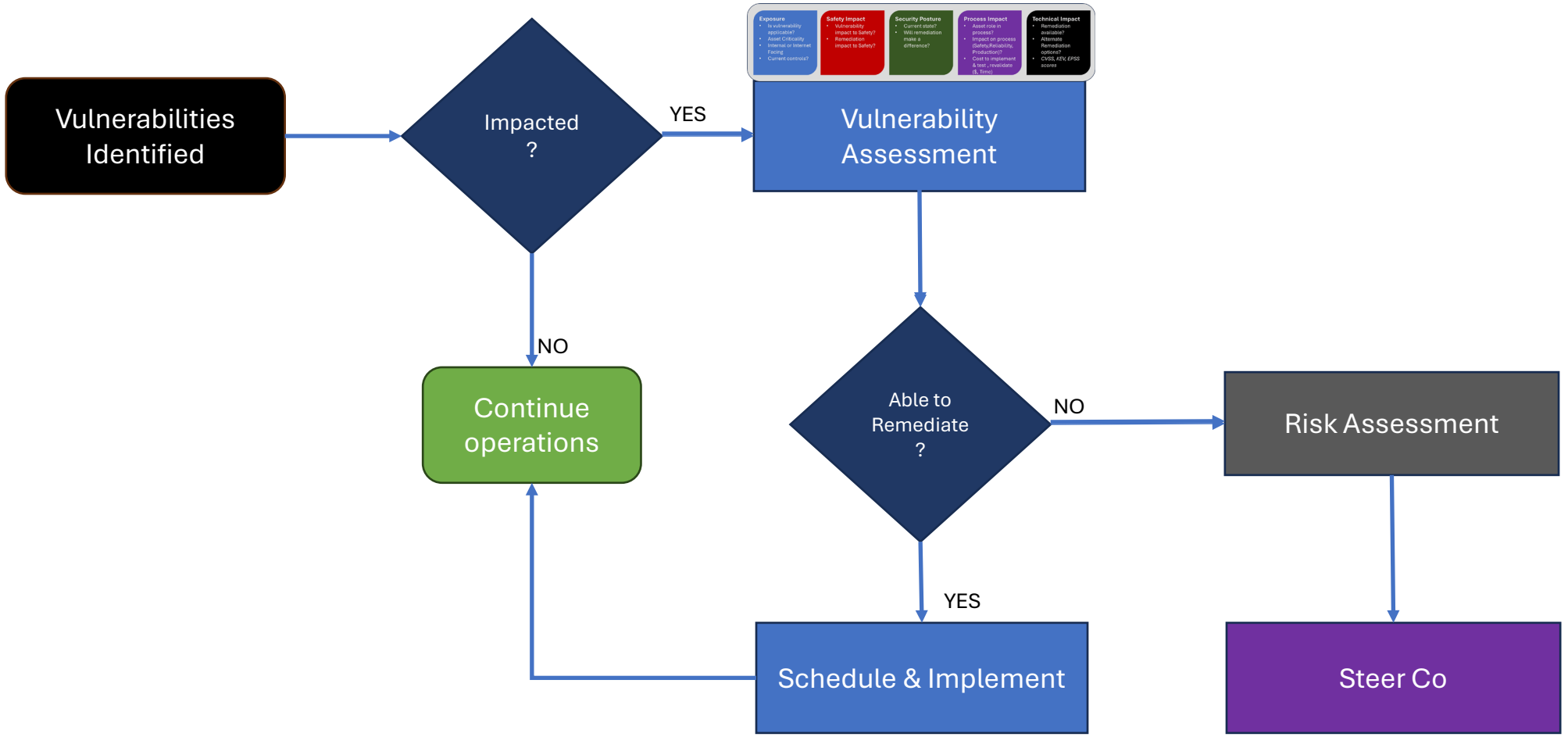


Verify & Report

- Verify change success
- Communicate and Report
- Architecture & baseline configuration updates
- Update docs & diagrams!!

Remember : ALL changes in OT & ICS environments pose risk which needs to be managed

Vulnerability Process Flow



Alternative Remediations – you can always do something which is better than nothing

RULE: Remediate as close to vulnerable system(s) as feasible

- Disable, remove service/component
- Firewall rules & network configuration
- Restrict/Reduce User access
- Increase OT Logging & Monitoring , Update Playbooks
- Architecture – segmentation, zones
- System Upgrades ($$$)

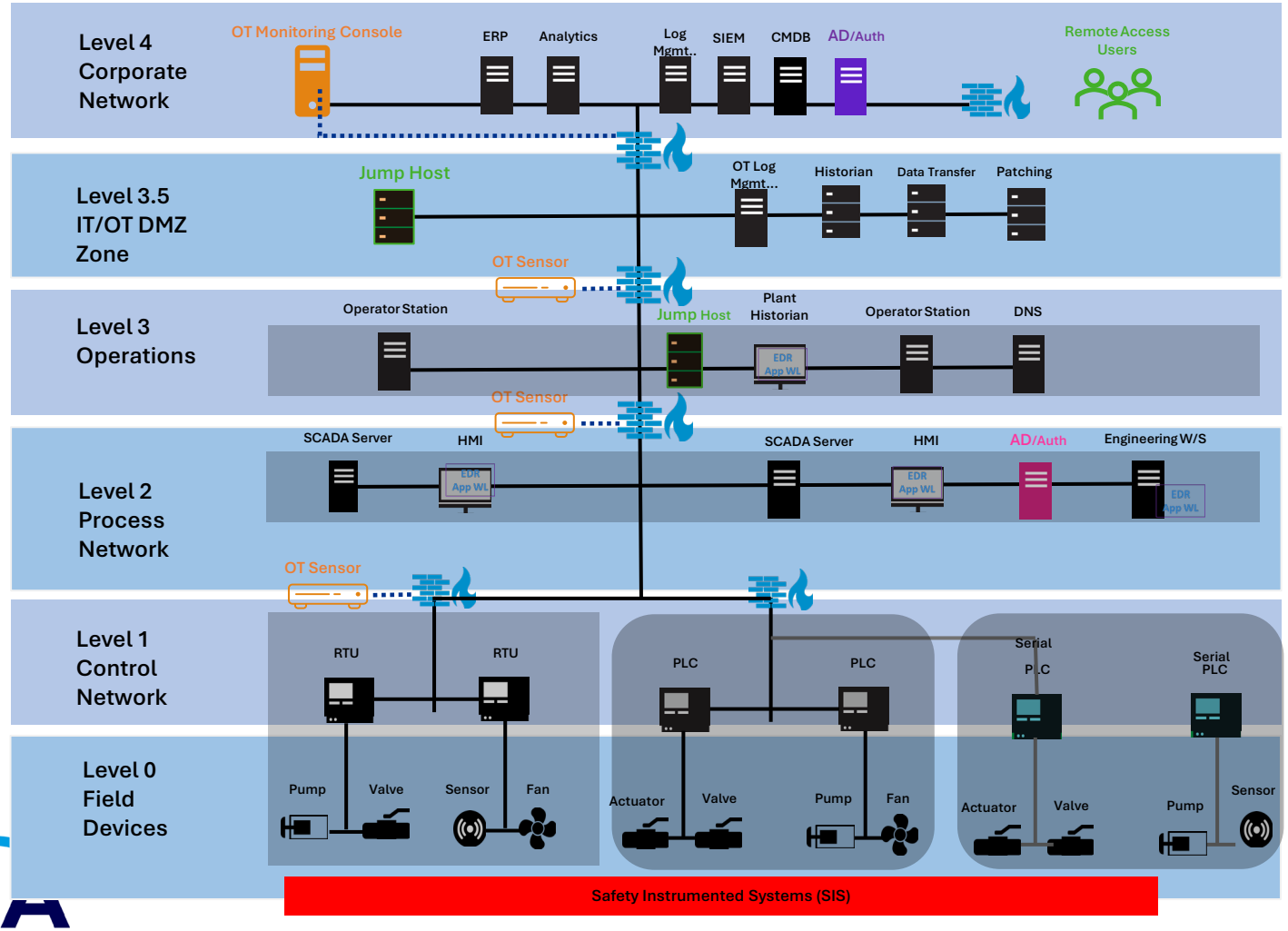
How can we reduce the workload & effort?

SANS – The Five ICS Cybersecurity Critical Controls

1 **ICS Incident Response Plan**	2 **Defensible Architecture**	3 **Network Visibility and Monitoring**	4 **Secure Remote Access**	5 **Risk-based Vuln. Management**
• Detect and contextualise threats • Establish Forensic capability • Response playbooks • Training & Exercises	• Establish defensible network architecture to support monitoring, response, reduce attack surface	• Continuous monitoring • Asset identification & Management • OT protocol aware • Integration with IT and OT teams	• Identification and inventory of *all* remote access methods • Connections monitored and recorded.	• Understand OT risks, context and drivers • Asset inventory • Establish risk-based vulnerability management program

Source: SANS.ORG https://sansorg.egnyte.com/dl/R0r9qGEhEe
Dragos : Dragos-5-Critical-Controls-OT-Cybersecurity-Guide-v1.pdf

The best Remediation … A defensible architecture



Traffic controls, Network Segmentation, inc. ZTNA

Zones and Conduits

Separate Identity & Access Management) + MFA

Continues Asset ID and Situational Awareness

Secure Remote Access + MFA

EDR / Application Whitelisting ?

Homework – next 90 days

30

- Updated asset inventory
- Identify stakeholders
- Identify critical assets
- Identify threat feeds/sources

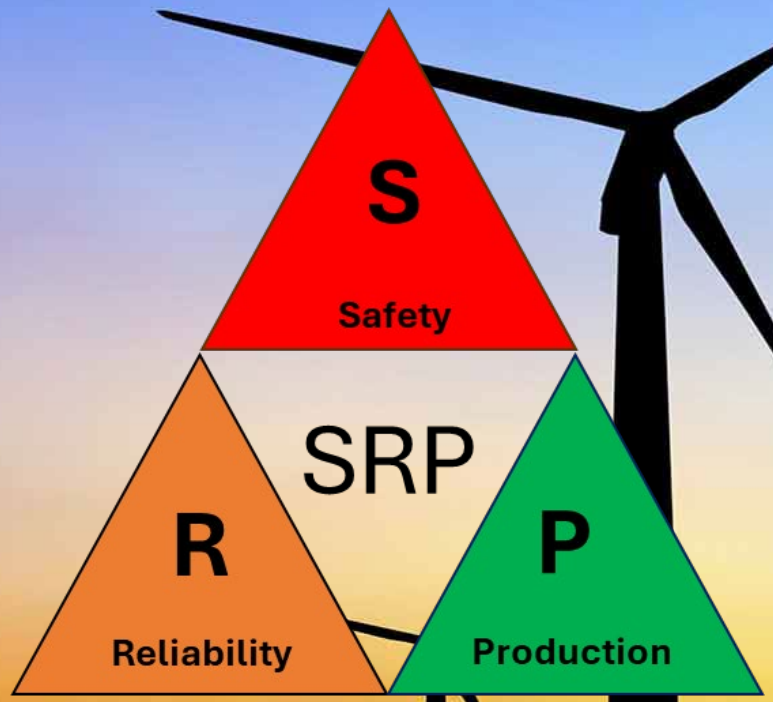
60

- Assess threats & risks
- Identify vulnerabilities
- Plan remediation
- Schedule remediation
- Monitor remediation progress

90+

- Establish governance
- Maintain vulnerability management processes
- Improve tooling
- Address architecture & baseline configurations

Thank You



OT Vulnerability Management is possible!

- Safety, Reliability, Production
- Governance is essential
- Planning & communication is key
- There is always some form of remediation available

camorrisaus
Infosecmorc