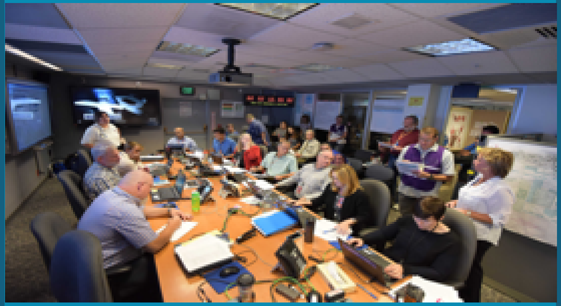
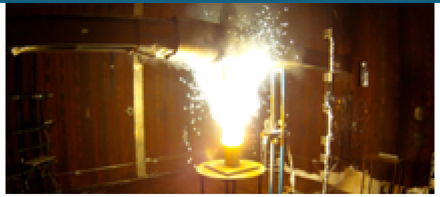
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

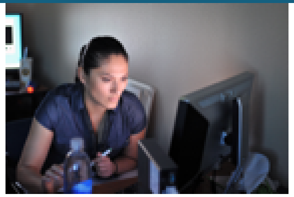
SAND2022-7643C

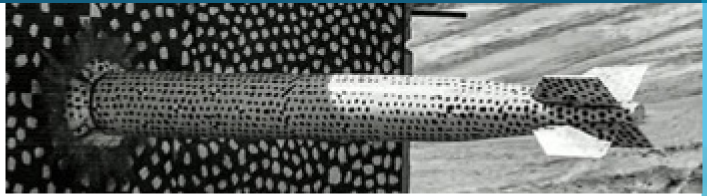
Sandia National Laboratories

MANAGING CYBERSECURITY SUPPLY CHAIN RISKS FOR THE SECURITY OF RADIOACTIVE SOURCES









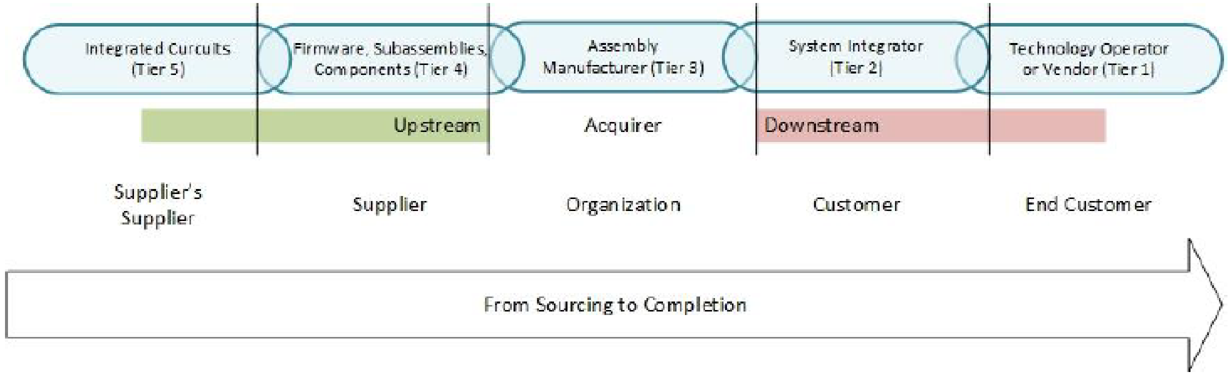
Michael T. Rowland

U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Supply Chain Relationships



Integrated Curcuits (Tier 5)

Firmware, Subassemblies, Components (Tier 4)

Assembly Manufacturer (Tier 3)

System Integrator (Tier 2)

Technology Operator or Vendor (Tier 1)

Upstream

Acquirer

Downstream

Supplier's Supplier

Supplier

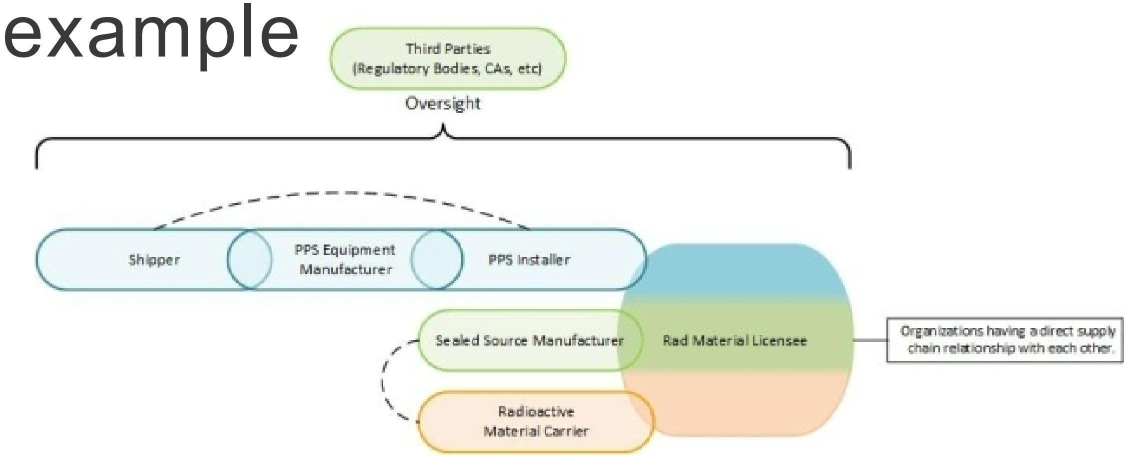
Organization

Customer

End Customer

From Sourcing to Completion

Radioactive source supply chain example



Third Parties (Regulatory Bodies, CAs, etc)

Oversight

Shipper

PPS Equipment Manufacturer

PPS Installer

Sealed Source Manufacturer

Rad Material Licensee

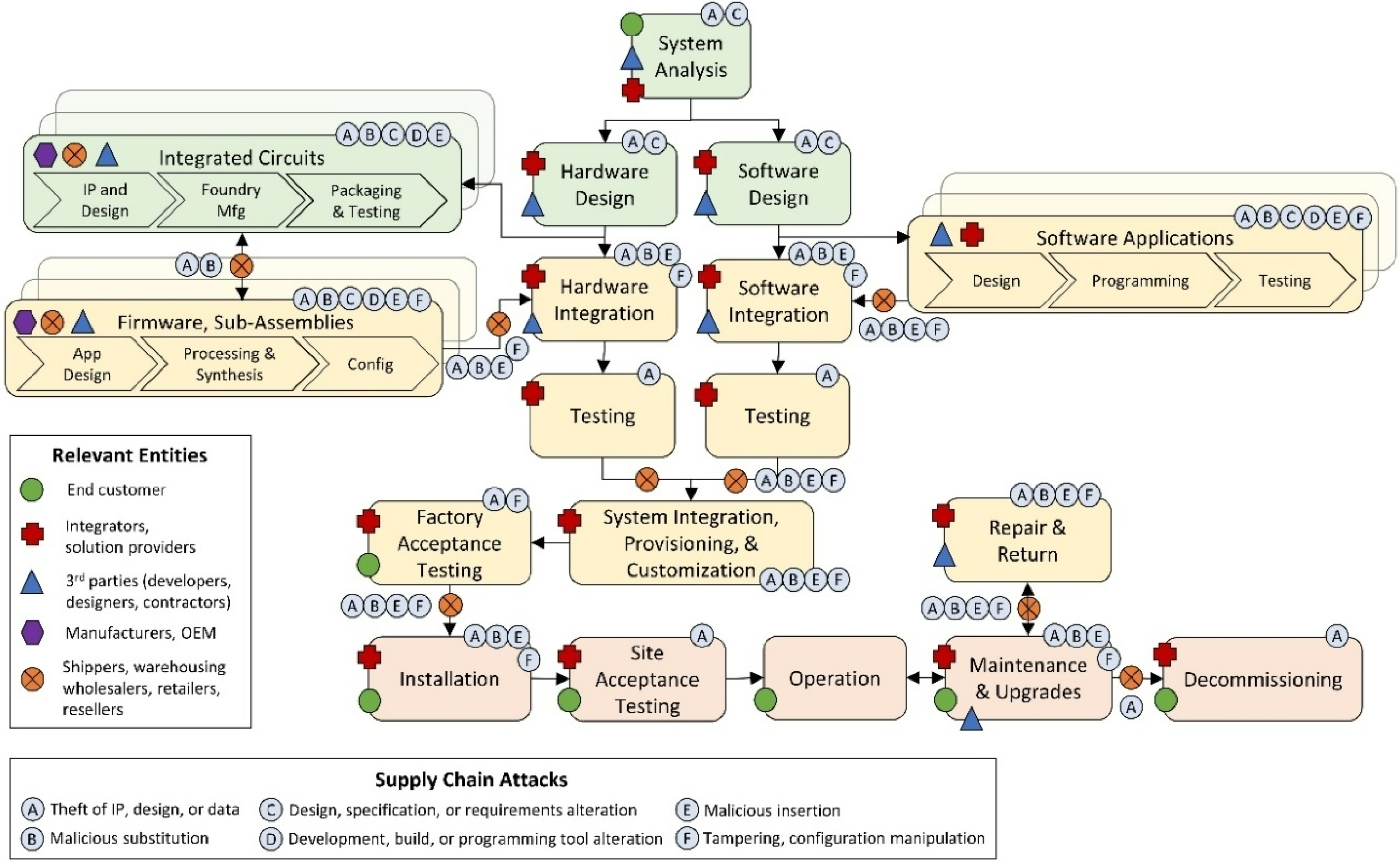
Radioactive Material Carrier

Organizations having a direct supply chain relationship with each other.

2 supply chains – PPS, radioactive source

PPS supply chain risk includes Shipper, PPS equipment MFG, PPS Installer and licensee(internal)

Attack surface (Example)



System Analysis A C

Hardware Design A C

Software Design A C

Integrated Circuits A B C D E
IP and Design
Foundry Mfg
Packaging & Testing

A B

Firmware, Sub-Assemblies A B C D E F
App Design
Processing & Synthesis
Config

A B E F

Hardware Integration A B E F

Software Integration A B E F

Software Applications A B C D E F
Design
Programming
Testing

A B E F

Testing A

Testing A

A B E F

Factory Acceptance Testing A F

System Integration, Provisioning, & Customization A B E F

Repair & Return A B E F

A B E F

A B E F

Installation A B E F

Site Acceptance Testing A

Operation

Maintenance & Upgrades A B E F

A

Decommissioning A

Relevant Entities

● End customer

✚ Integrators, solution providers

▲ 3rd parties (developers, designers, contractors)

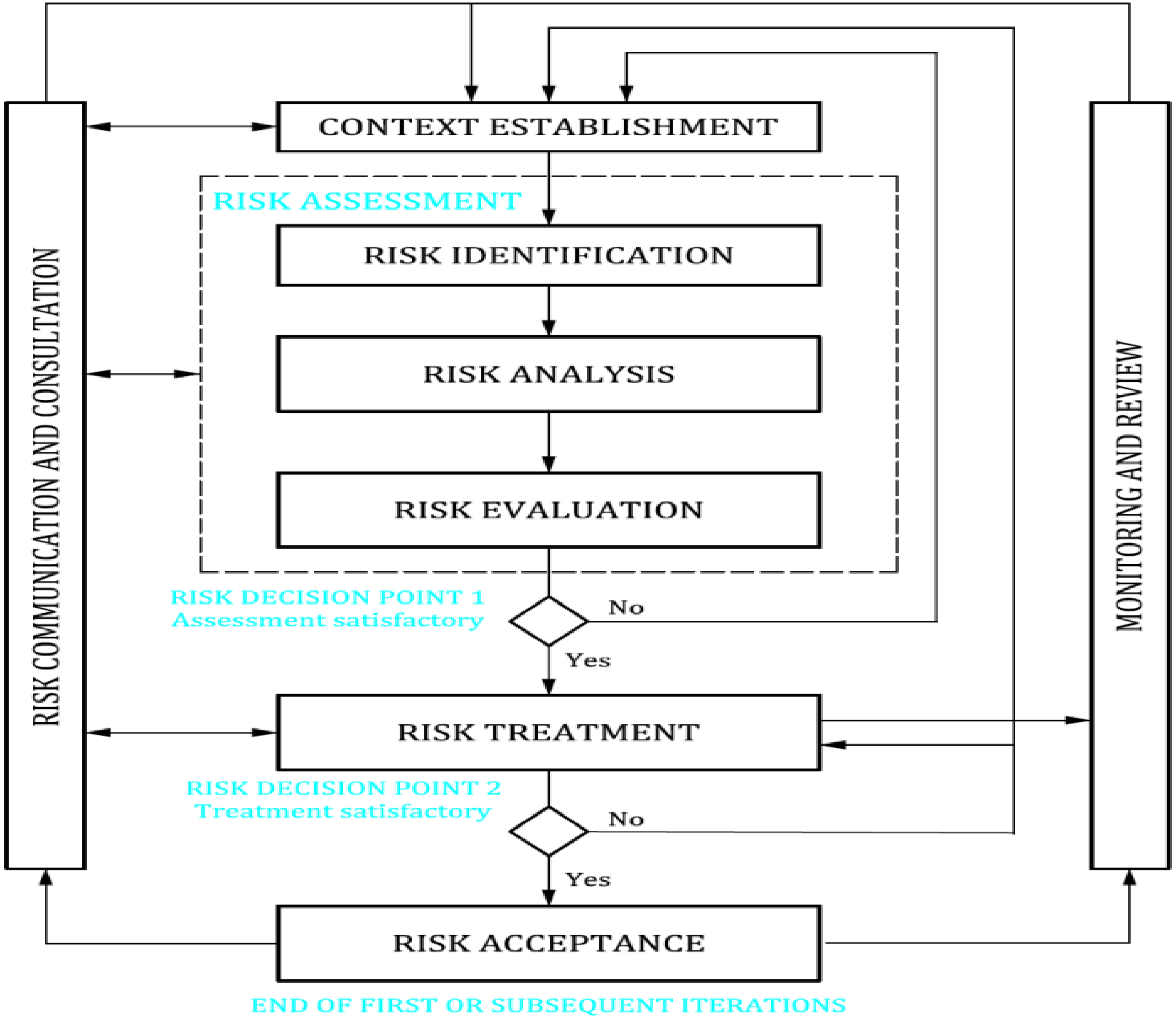
⬢ Manufacturers, OEM

⊗ Shippers, warehousing wholesalers, retailers, resellers

Supply Chain Attacks

Ⓐ Theft of IP, design, or data	Ⓒ Design, specification, or requirements alteration	Ⓔ Malicious insertion
Ⓑ Malicious substitution	Ⓓ Development, build, or programming tool alteration	Ⓕ Tampering, configuration manipulation

Risk Management (ISO/IEC 27005:2018)



Hypothetical example PPS GULA Hospital

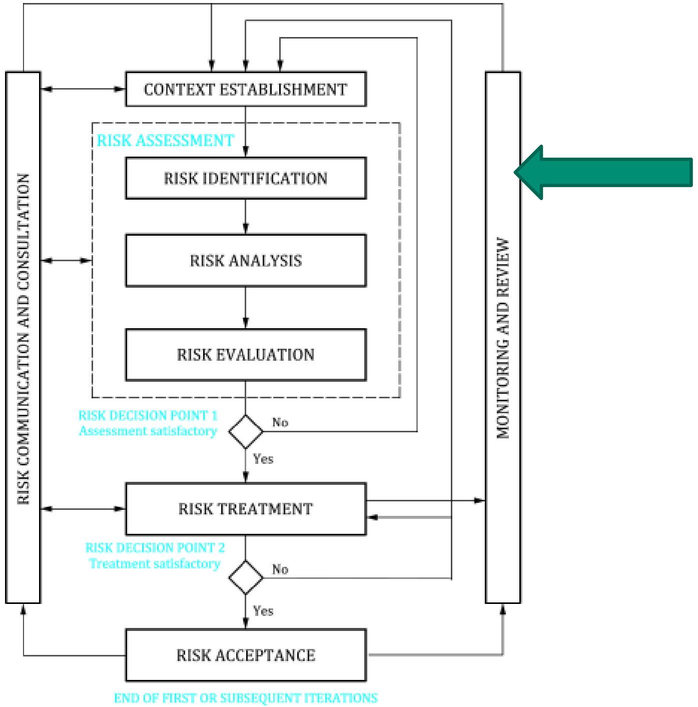
A digital physical protection system (PPS) provides for security of the radioactive material.

- The radioactive source is used for blood irradiation and is located in the basement of the hospital.
- The PPS provides protection of this irradiator and alerts to a security monitoring room.
- The PPS is connected through a firewall to the site security system which then backs up key data to a cloud storage service.

Incident Scenario for Risk 1

In this scenario, the adversary is aiming to disable the PPS through ransomware attack. This involves compromise of a PPS maintainer that has physical access to the PPS and performs updates by directly connecting a mobile device. The initial step is compromised of the maintenance supplier’s networks via phishing attack. This provides the adversary with information on the PPS configuration and design as well as the schedule for maintenance activities. The adversary is then able to confirm vulnerabilities on the PPS that would allow for the installation of ransomware via the mobile device connection. The adversary waits until the ransomware is installed and then plans to commence a physical attack once the PPS is disabled.

Hypothetical example PPS GULA Hospital Risk Identification



CONTEXT ESTABLISHMENT

RISK ASSESSMENT

RISK IDENTIFICATION

RISK ANALYSIS

RISK EVALUATION

RISK DECISION POINT 1 Assessment satisfactory

No

Yes

RISK TREATMENT

RISK DECISION POINT 2 Treatment satisfactory

No

Yes

RISK ACCEPTANCE

END OF FIRST OR SUBSEQUENT ITERATIONS

RISK COMMUNICATION AND CONSULTATION

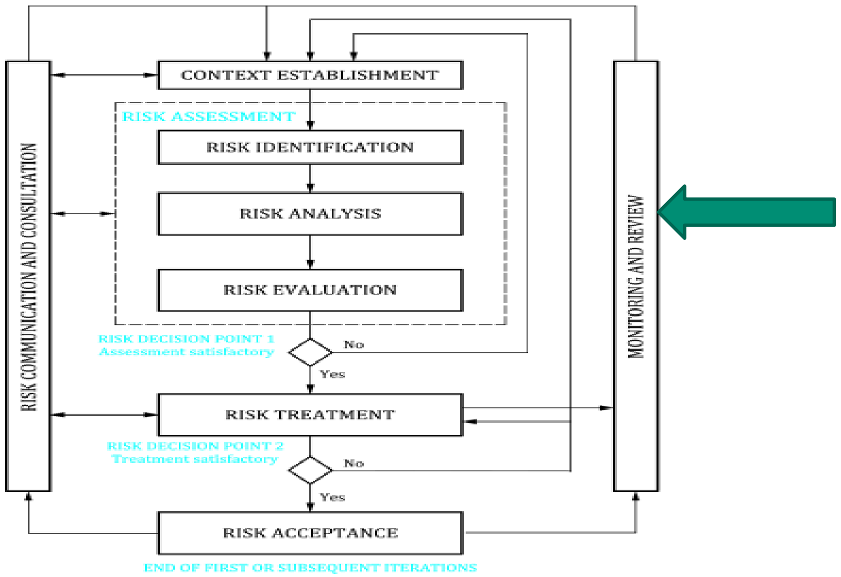
MONITORING AND REVIEW

- Threats to Supply Chain can be present in vulnerabilities of acquired product
- Risks can be inherited from upstream in the supply chain

Risk No	Products/Services	Risk Type	Description of Risk	Applicability to PPS
1	Acquisition of Products	Information Security Feature	Acquirer’s derived products, services, or processes vulnerable due to a supplied product’s vulnerability	Vulnerability in the PPS HMI display software could allow for unauthorized disabling of alarms

For Brevity we follow Risk ID 1

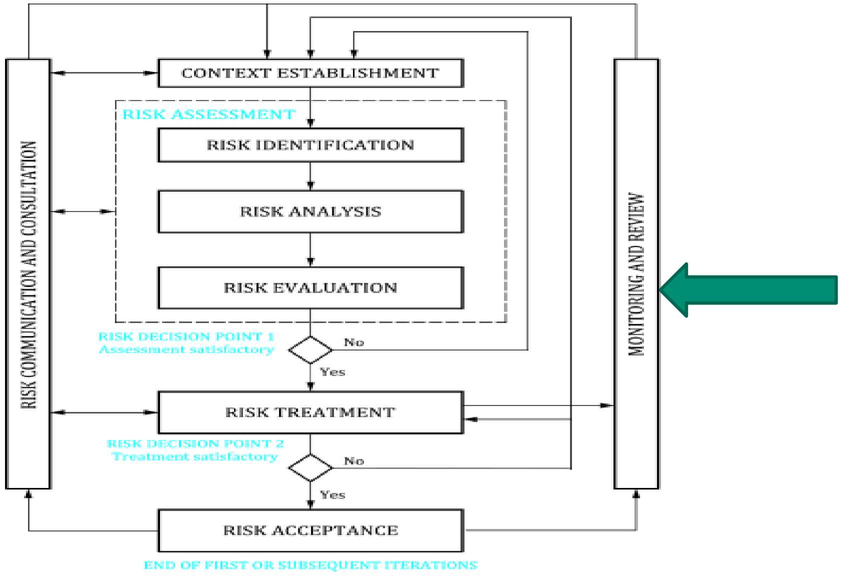
Scenario Risk (1) Risk Analysis



- Qualitative and quantitative risk methodologies are considered
- Assessment of likelihood

Risk No.	Risk Type	Identified Risk	Likelihood	Consequence
1	Information Security Feature	Attackers use maintenance on the PPS HMI to disable PPS.	Low Phishing and ransomware attacks highly probable. However, leveraging these attacks to target PPS of other RM have yet to be reported.	Low The PPS system fails secure, so an attempt to completely disable the system would not provide access. The failure is detected in a relatively short period of time and the compensatory actions are known (e.g., guards at entry points).

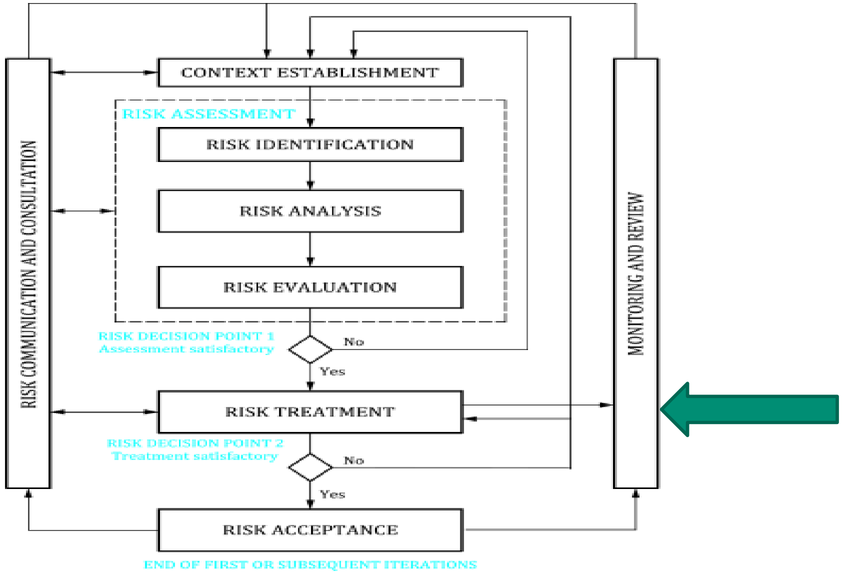
Risk Evaluation and Prioritization



- Risk priority may change as additional risks are identified, or as conditions change

- Once all identified risks have been analyzed list risks based on that analysis
- Determine priority
- Generally its expected the severity of consequence will remain constant for each risk but the likelihood of the scenario may vary
- In our example Risk 1 listed in this presentation was evaluated as priority 3

Risk Treatment



RISK COMMUNICATION AND CONSULTATION

CONTEXT ESTABLISHMENT

RISK ASSESSMENT

RISK IDENTIFICATION

RISK ANALYSIS

RISK EVALUATION

RISK DECISION POINT 1
Assessment satisfactory

No

Yes

RISK TREATMENT

RISK DECISION POINT 2
Treatment satisfactory

No

Yes

RISK ACCEPTANCE

END OF FIRST OR SUBSEQUENT ITERATIONS

MONITORING AND REVIEW

Risk Transfer

- Contractual requirements (external)
- Policy or Organizational requirements (internal)

Risk Modification

- Knowledge based detection
  - Known malware, vulnerabilities
- Behavior –based detection may require continuous monitoring
  - Cyber SOC, host based intrusion

In our example risk walkthrough, Risk 1 treatment includes passwords, remote access controls and audits (TRANSFER) AND

Risk Modification – Patches, defensive architecture elements that limit or mitigate the attack pathway

Defense-In-Depth conclusion

This approach applies a graded approach (security levels)

Implement defense-in-depth (diversity, independence)

Improve

- Identification of risks
- Analysis of those risks and potential impacts to security of radio active sources
- Evaluation of risks to prioritize through countermeasures

Case Study

Solar Winds – SUNBURST Attack

https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

Thank you!