

# Engineering Safety and Security in the era of the Industrial Internet of Things



Dr Robert Oates

© 2017 Rolls-Royce plc

The information in this document is the property of Rolls-Royce plc and may not be copied or communicated to a third party, or used for any purpose other than that for which it is supplied without the express written consent of Rolls-Royce plc.

This information is given in good faith based upon the latest information available to Rolls-Royce plc, no warranty or representation is given concerning such information, which must not be taken as establishing any contractual or other commitment binding upon Rolls-Royce plc or any of its subsidiary or associated companies.

Trusted to deliver excellence

Private – Rolls-Royce Proprietary Information



Rolls-Royce

# Talk Structure

- **Who am I?**
- **What is Product Cyber Security?**
- **Why is it important to understand the interactions between safety and security?**
- **How do safety and security interact?**



# Product Cyber Security Team



# Rolls-Royce

Civil  
Aerospace

Defence  
Aerospace

Marine

Nuclear

Power  
Systems

Product Cyber Security Team



Process  
Improvement



Auditing



Standardisation  
&  
Best Practice



Tooling



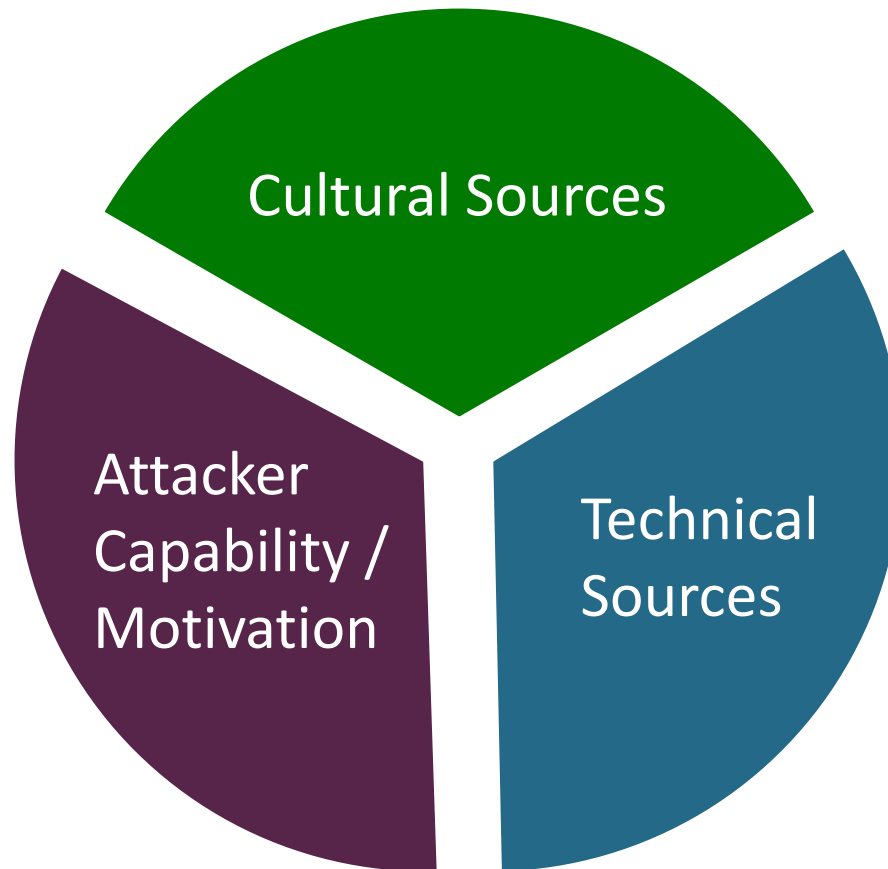
Project  
Support



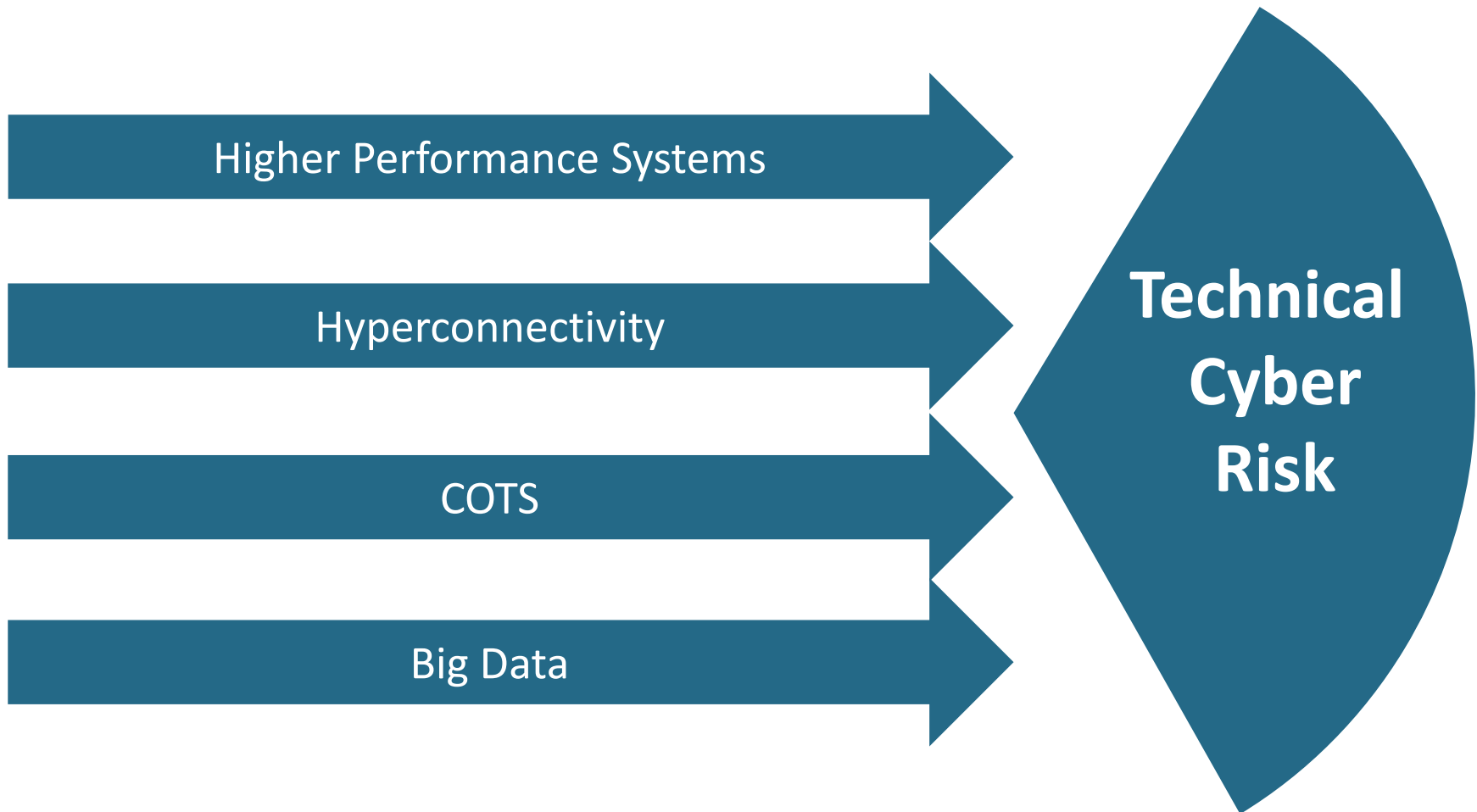
**Rolls-Royce**



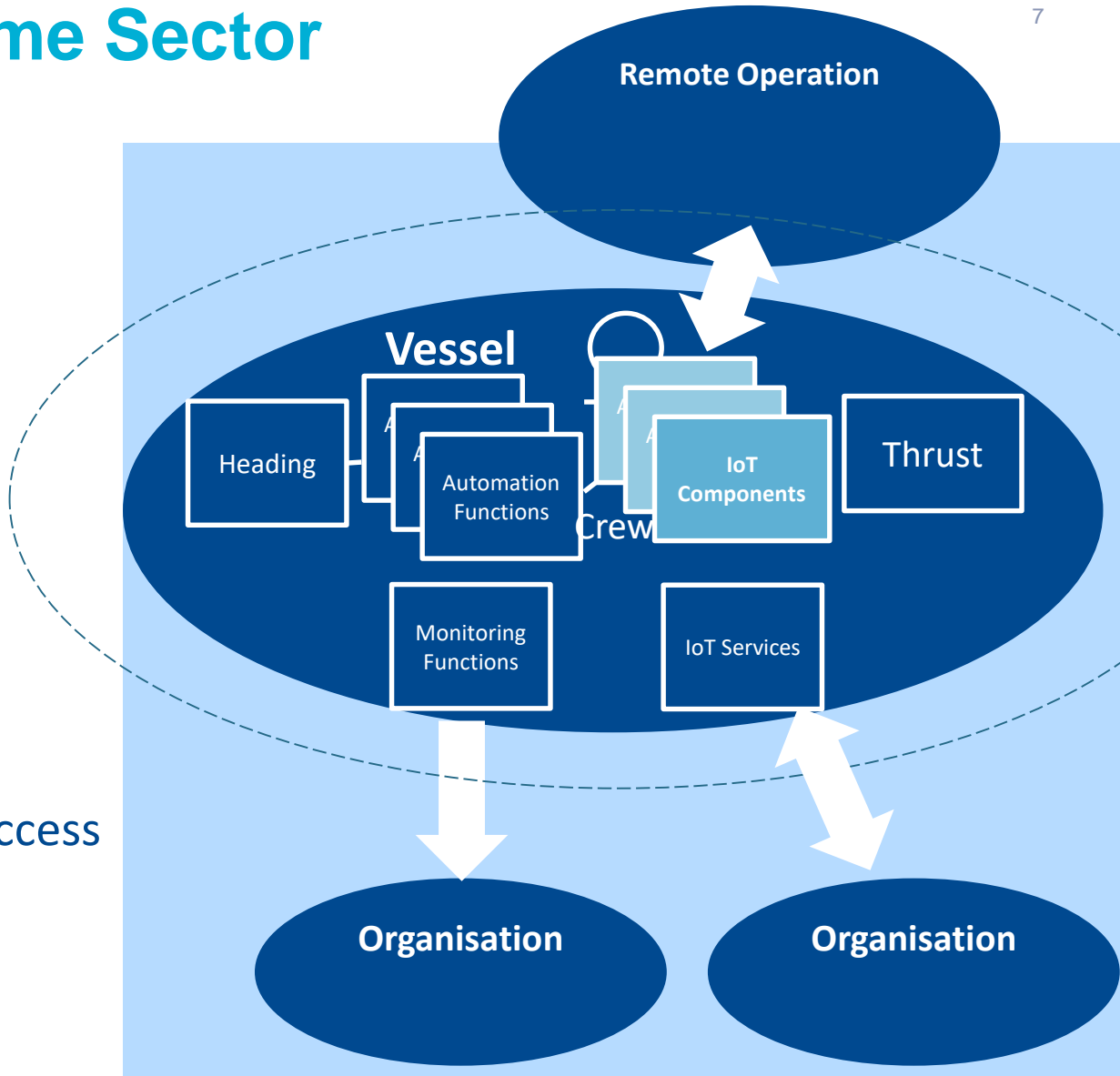
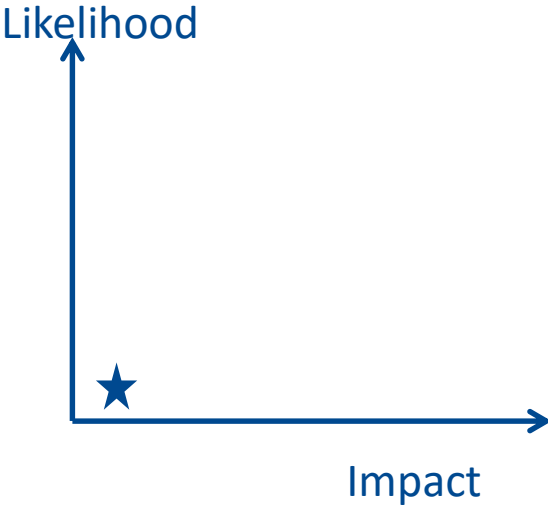
# Sources of Product Cyber Security Risk



# Technical Sources of Risk



# Example: Maritime Sector



- Data driven services
- Wireless sensor networks
- Automation and remote access
- Internet of Things



# Attacker Capability – Who is attacking?

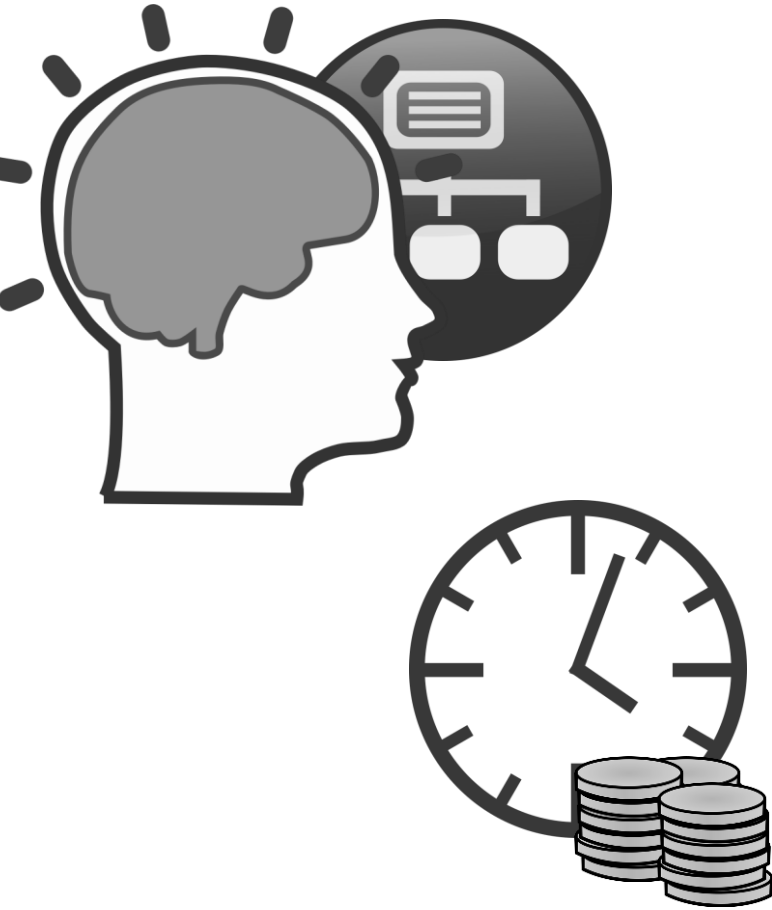
## CNI Attackers (From GAO):

- Nation states
- Terrorists
- Industrial spies and organised crime
- Hacktivists
- Hackers

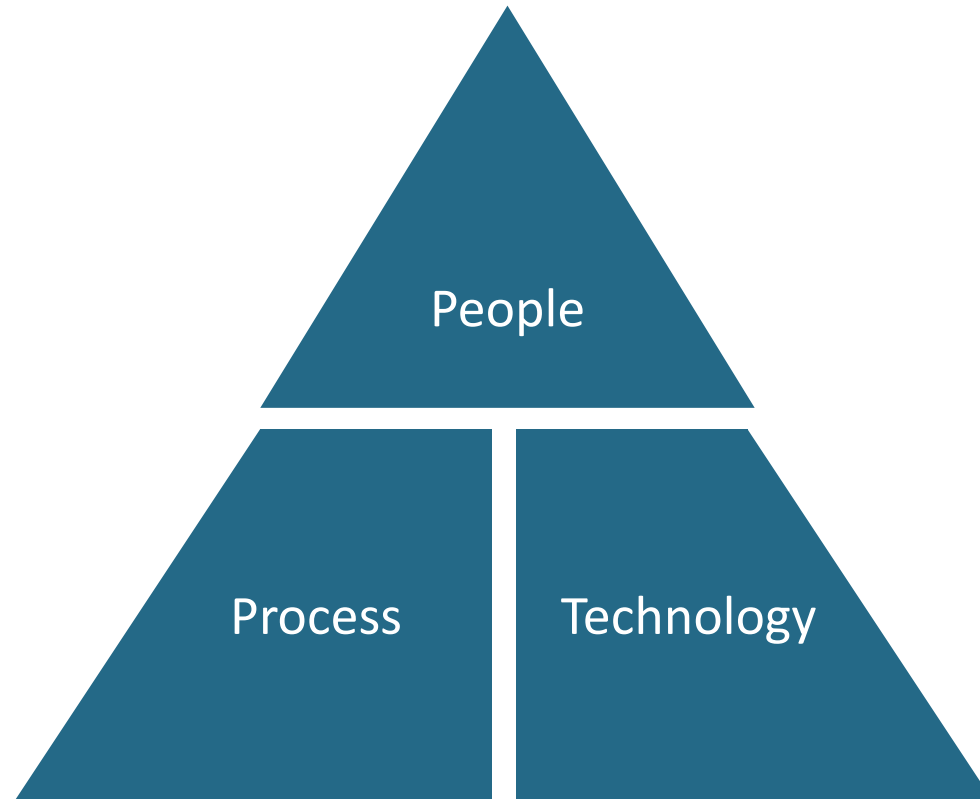




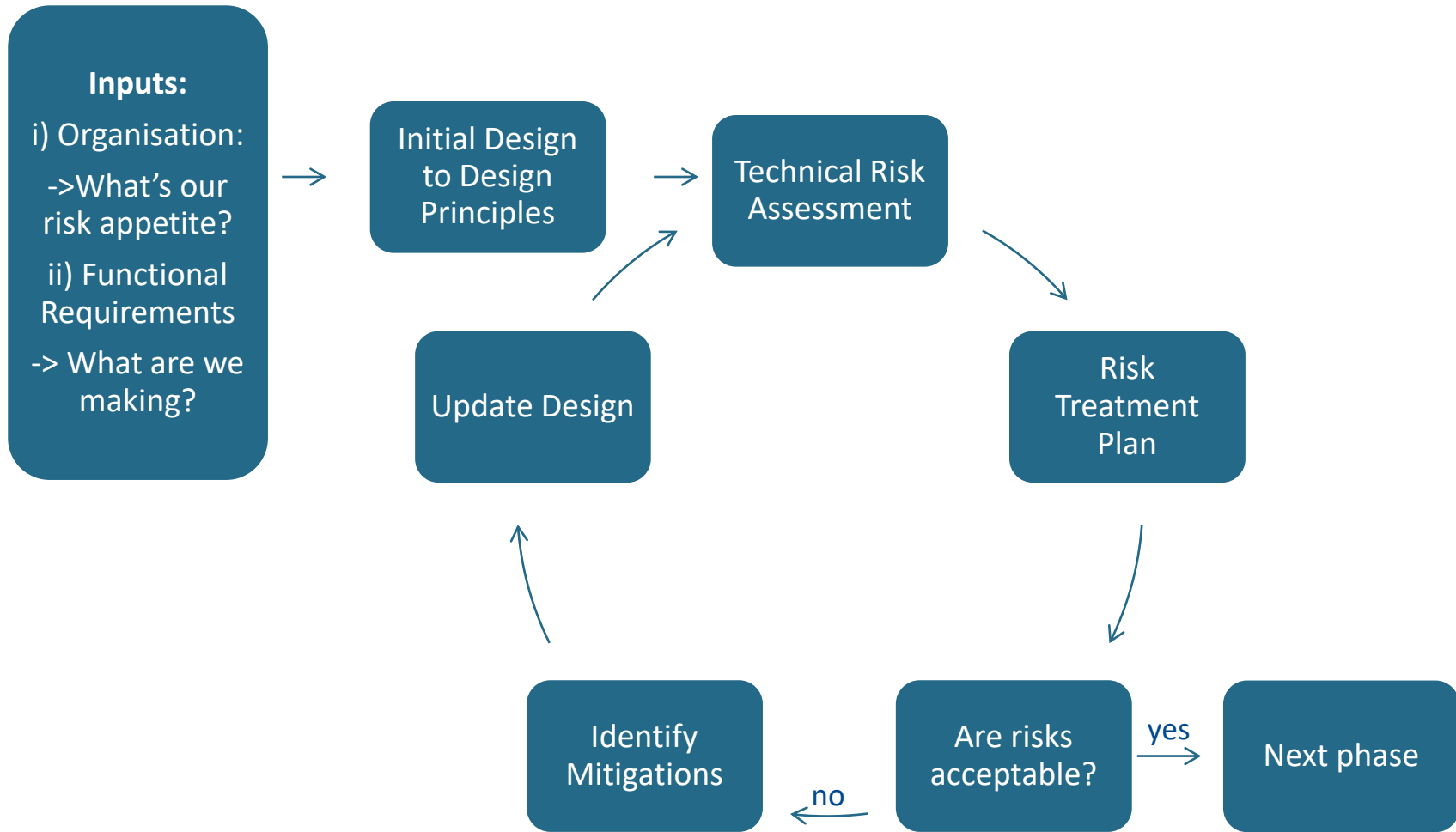
# Attacker resources



# What can we do about PCS Risk?



# Risk Driven Design Processes



# Secure Development Objectives



Security requirements across all sub systems to ensure that the system is secure at the system level

The argument that the system is secure, through life

Active security features/subsystems that detect and react to intrusions



# Changing Cultures

**Security is everybody's responsibility**



Training

Routes to escalation

Incident response planning

Security Champions

Communication



# Changing Cultures

## Proportionate, risk-based controls



Keep costs down

Keep risks down

Understand risk



Risk

Cyber  
Security

Safety

Economic

Attacks

Accidents

Financial  
Loss



# Statement 1

**Product cyber security is a risk source that needs to be addressed**





# Fundamental Question

Can a software intensive system be  
deemed **safe** if it isn't **secure**?



# The Enemies of Safety / The Results of Attacks

**Non-determinism**

**Uncontrolled change**

**Poor communication/understanding**



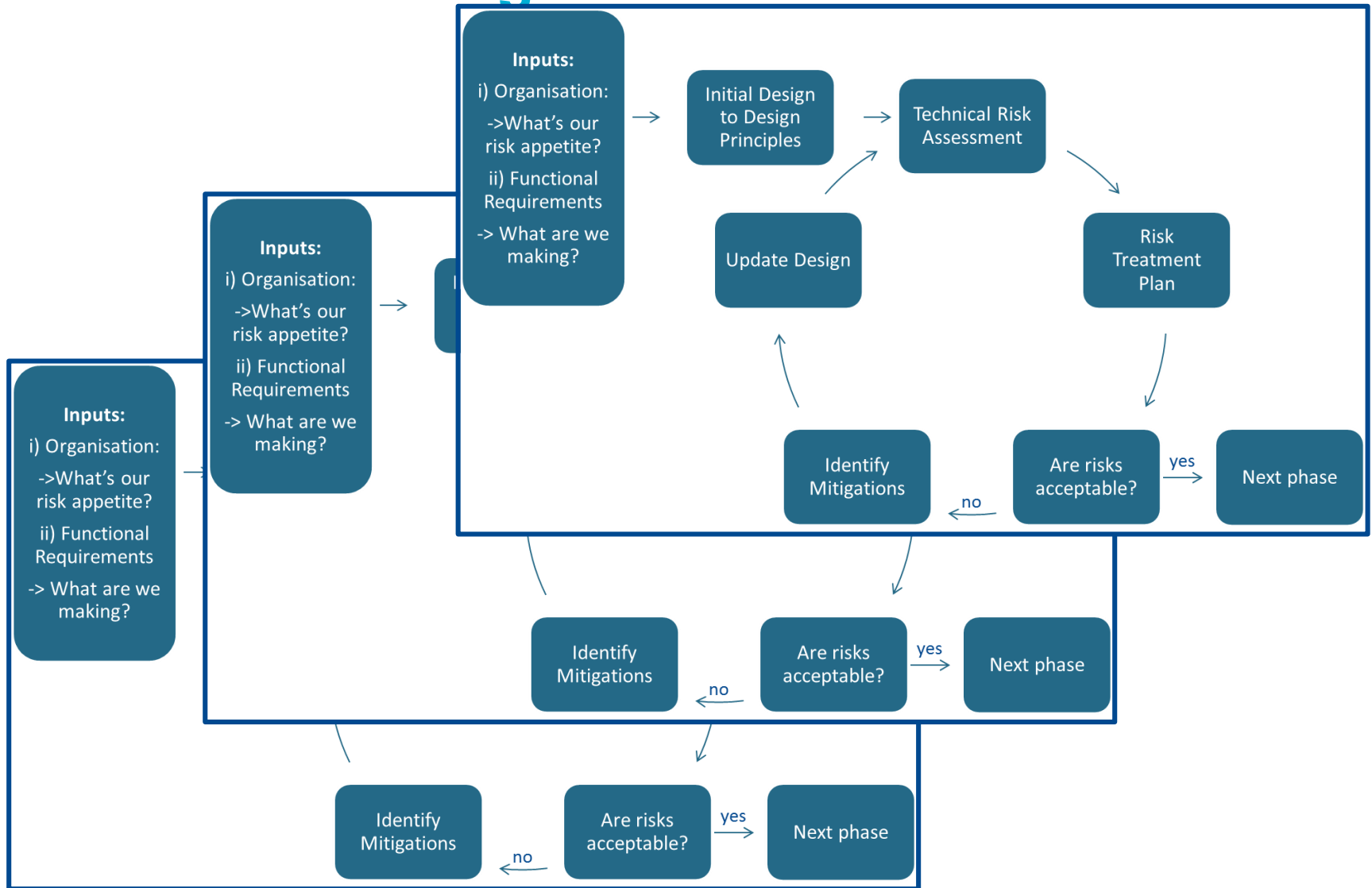
**SAFETY**

**≠ SECURITY**

**CRYPTO**



# Risk Driven Design Processes



# Statement 2

## Understanding the link to safety can make things

1. Safer
2. More secure
3. Cheaper

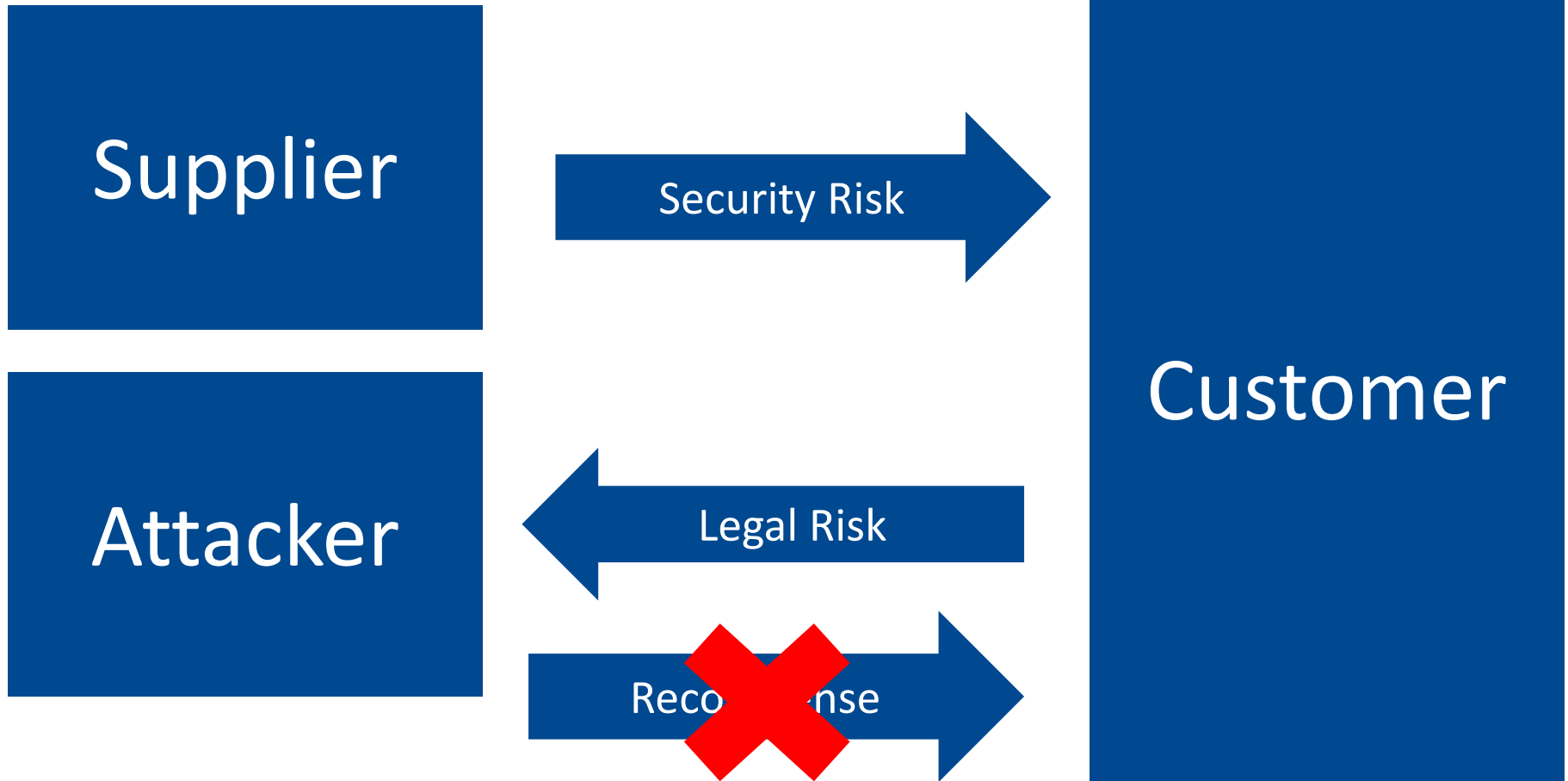




# Risk Direction: Safety



# Risk Direction: Security

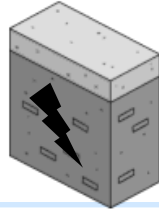




# Patching safety critical systems

*Discovery*

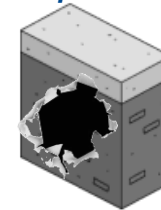
**Vulnerability  
Researcher**



**Malicious  
Actors**



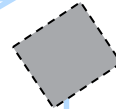
*Exploitation*



**Supplier**



*Patch creation*



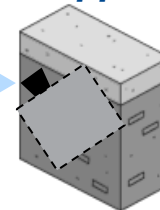
**System  
Integrator**

*Remedial  
actions*



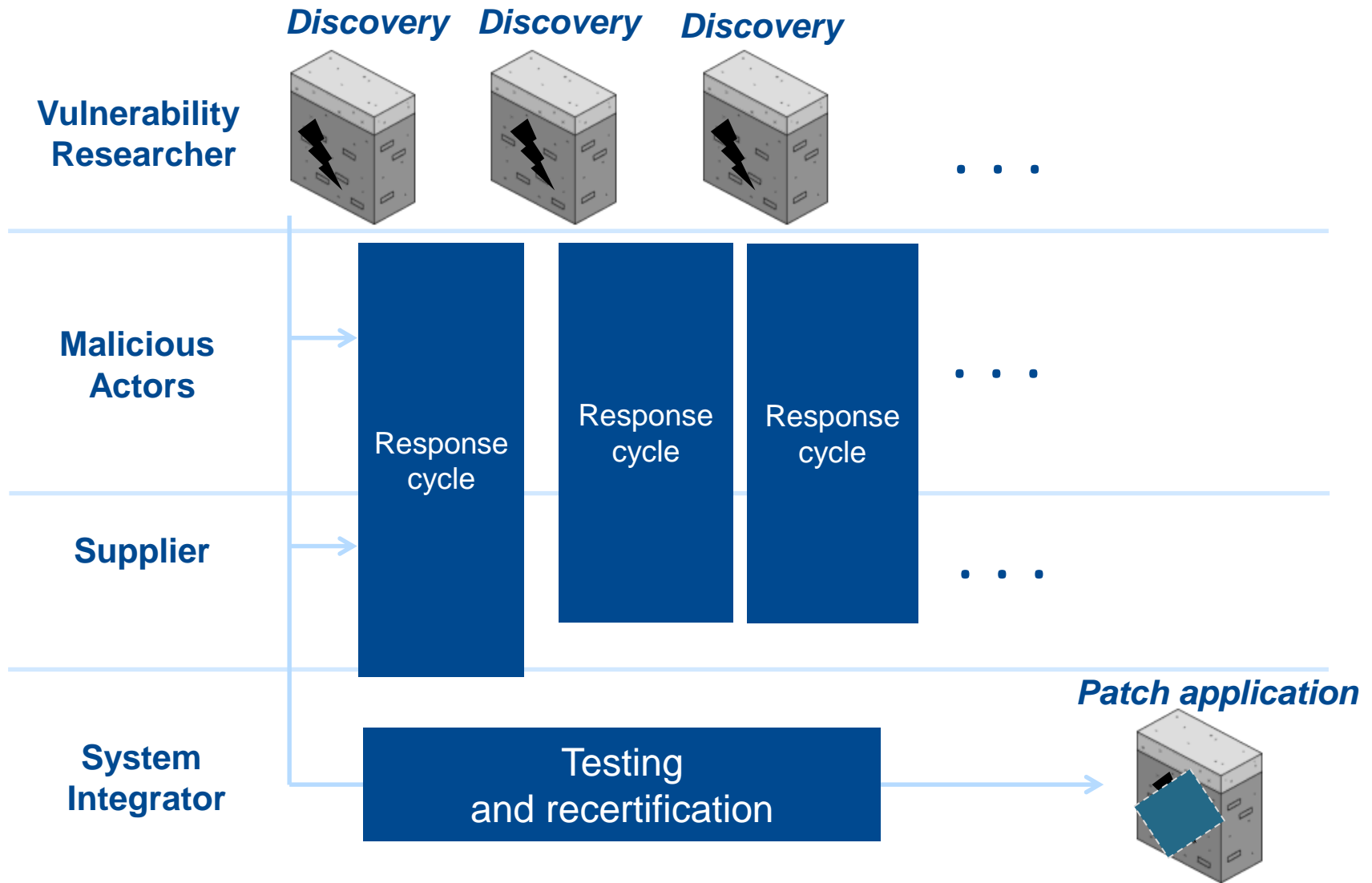
**Testing  
and  
recertification**

*Patch application*



**Rolls-Royce**

# Patching safety critical systems



# Design Principles in Opposition: Diversity

## Safety

$$P(\text{failure}) = (P(\text{failure of one component}))^2$$

Uncertainty: Low, de-risked from extensive testing and well established process

**Extremely Low risk system**

## Security

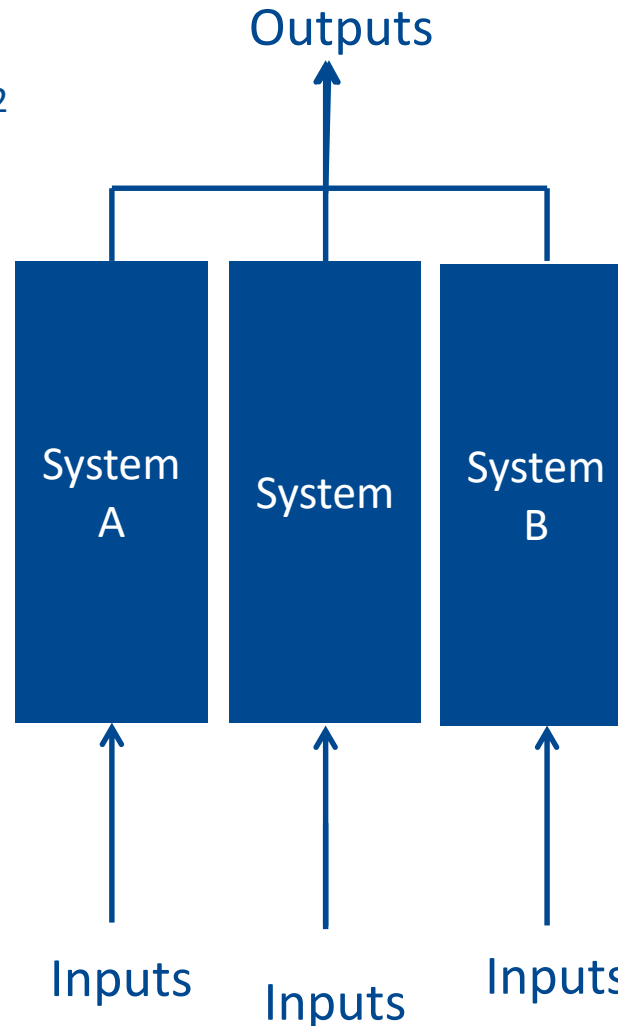
Likelihood of attack?

Implementation specific vulnerabilities **X**

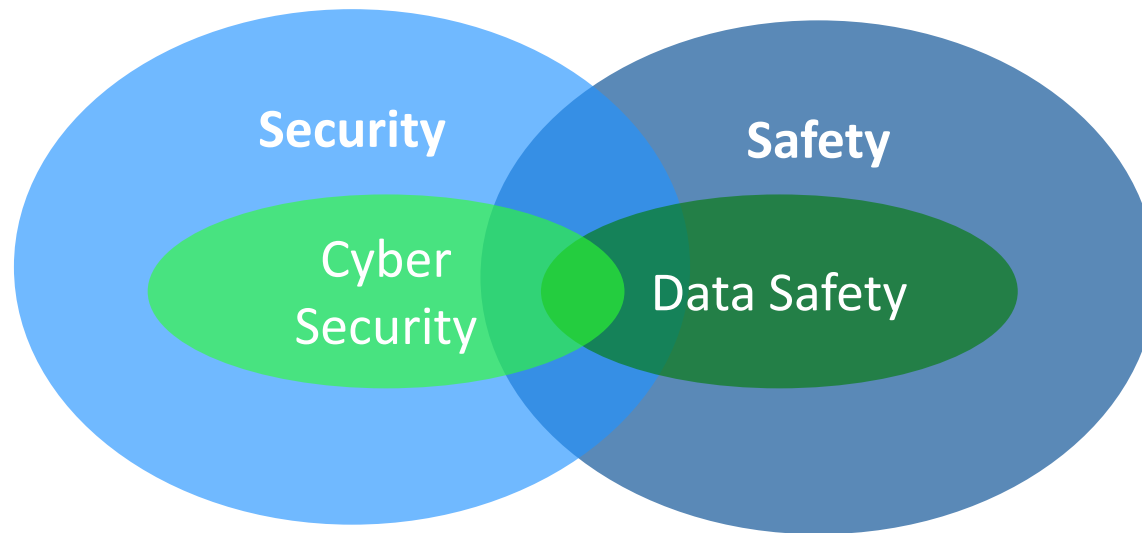
Specification vulnerabilities

Component vulnerabilities

**Risky system!**



# Understanding Risk



- System level quality factors
- Through life quality factors
- Preventing harm
- Design principles
- Risk driven design change
- Controls that are proportionate to risks

## Resist

### Network architecture

- Interface control
- Firewalls
- Data diodes
- Segregation

### Protocol Selection

### Cryptographic techniques

- Cryptographic agility – quantum!
- Legal issues

### Multi-source localisation

### Manual override

## Detect and React

### IDS

- What is normal?
- Interaction with watchdogs
- Does  
“Adaptive” = “Non-deterministic” ?

### Logging

- Review processes

### Reactions

- Security responses shouldn't compromise safety
- Safety responses shouldn't compromise security

**...but there are things missing.**

## **Systems Engineering for Safety and Security**

- Is a truly common risk model possible?

## **Efficient Incident Response**

- Design for Forensics
- Team members

## **Intelligence Focus**

- Where do you get threat intelligence from?
- How do you embed live intelligence into an engineering/maintenance process?



# Statement 3

**The interactions are complex. Some solutions exist,  
but there is a way to go**



# In Conclusion

- 1. Product cyber security is a risk source that needs to be addressed**
- 2. Understanding the link to safety can make things**
  1. Safer
  2. More secure
  3. Cheaper
- 3. The interactions are complex, solutions exist but there is a way to go**

