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

Dr Robert Oates

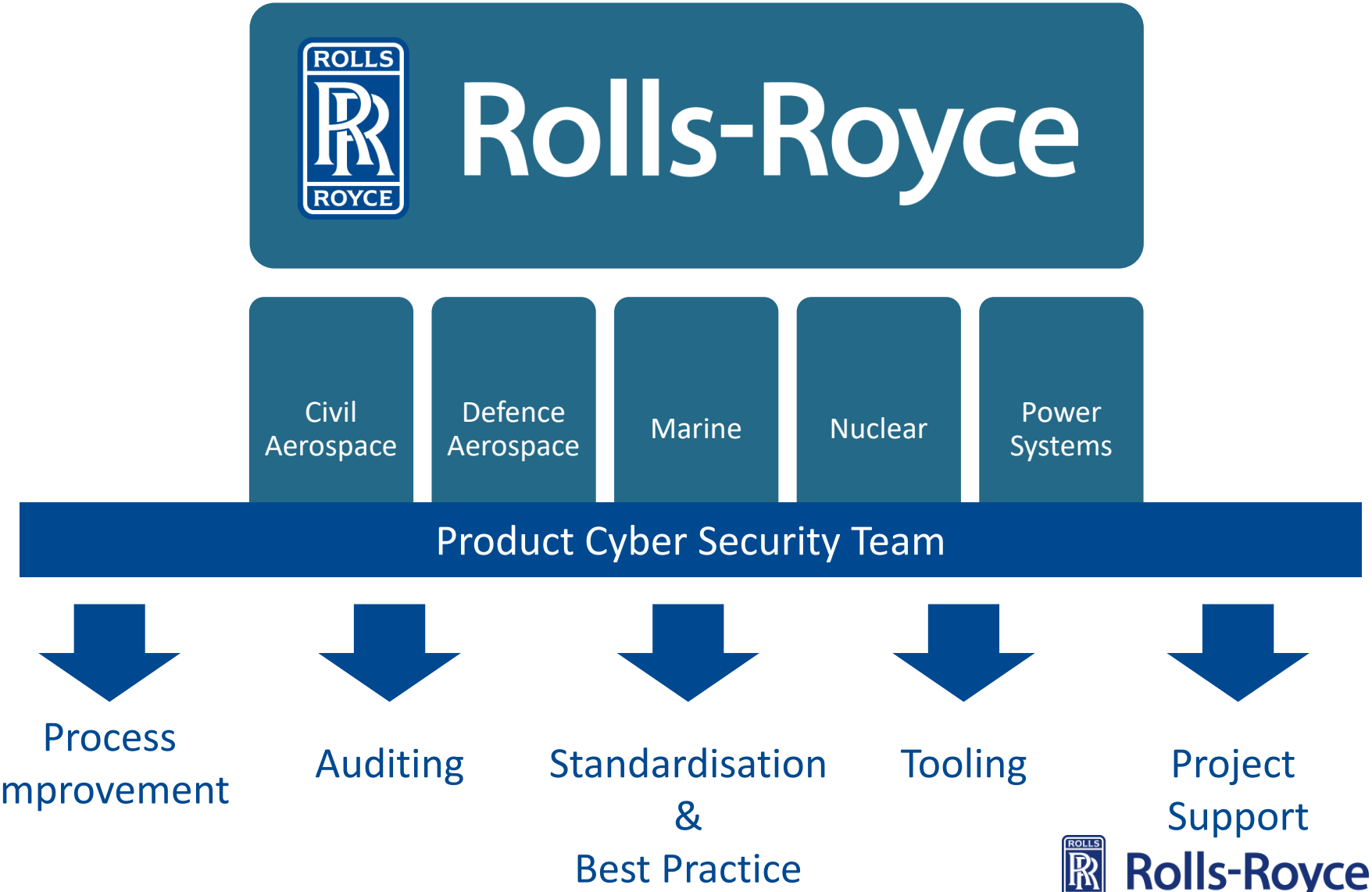
Trusted to deliver excellence

Rolls-Royce

Talk Structure

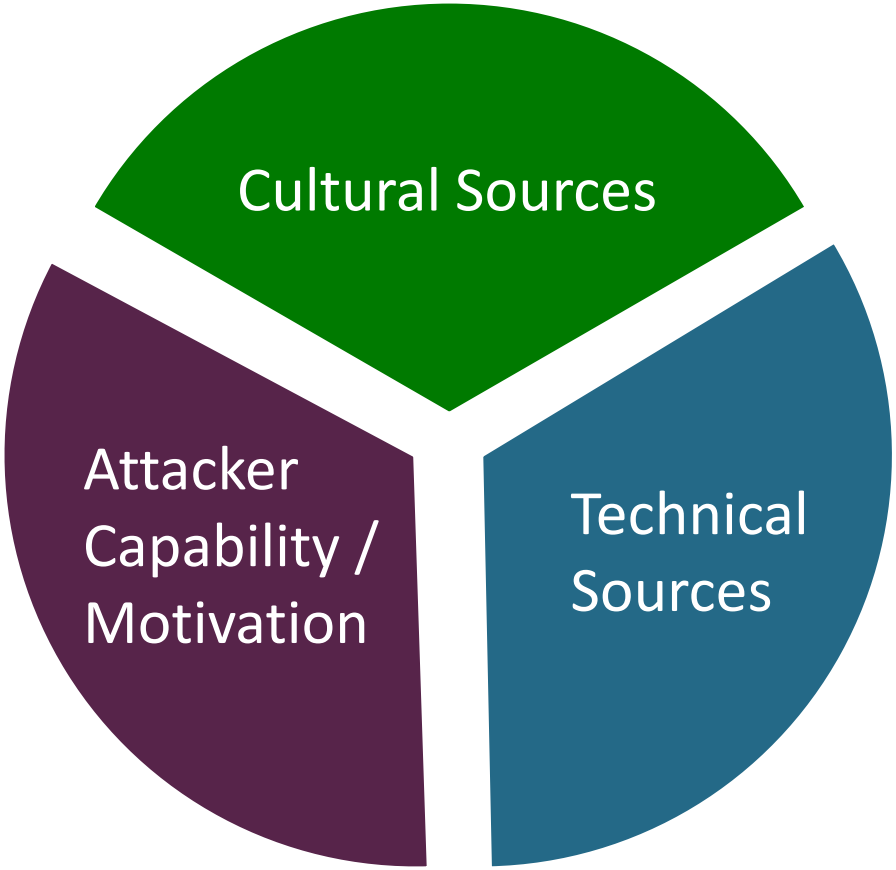
- **Who am I?**
- **What is Product Cyber Security?**
- **Why is it important to understand the interactions between safety and security?**
- **How do safety and security interact?**

Product Cyber Security Team

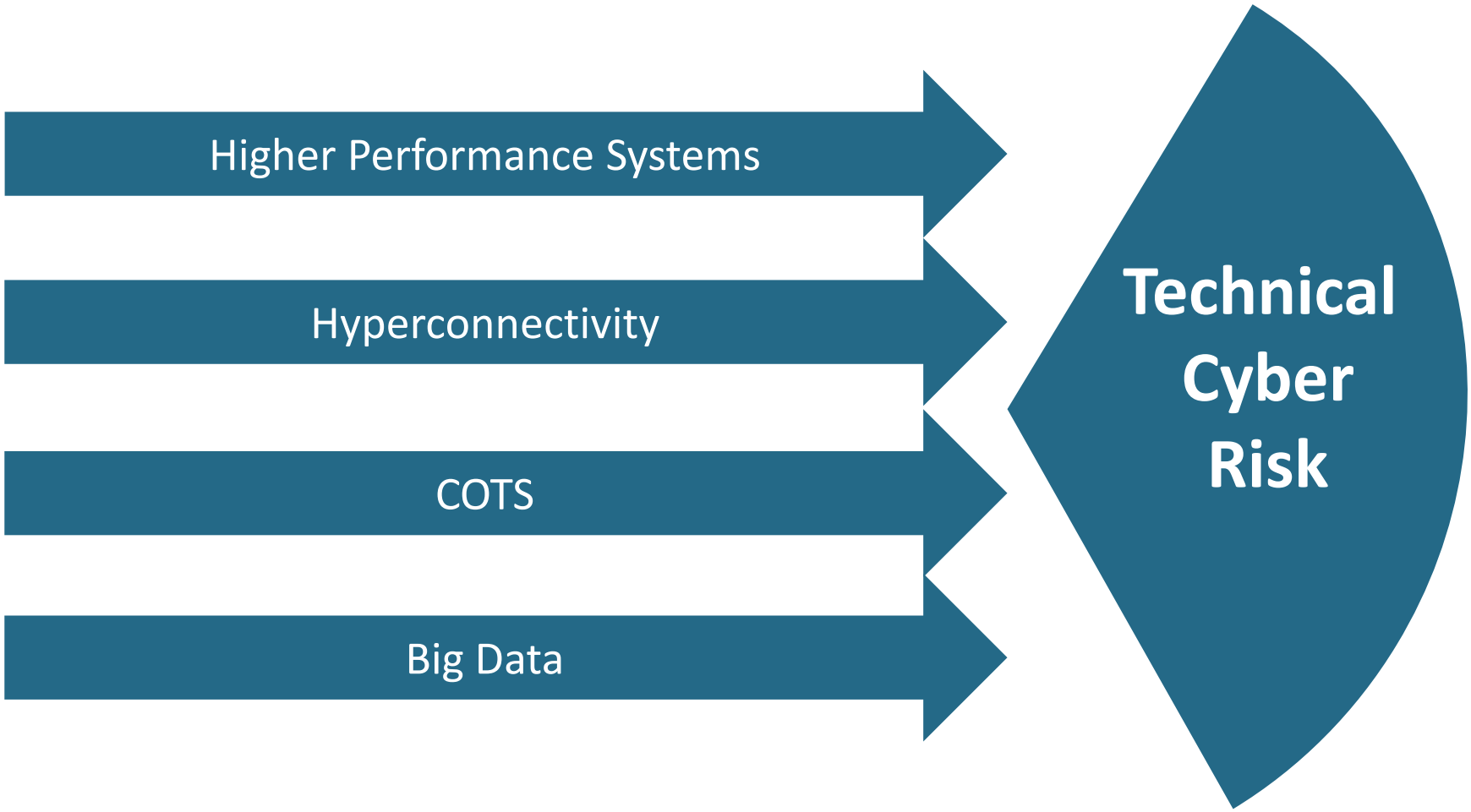


Rolls-Royce

Sources of Product Cyber Security Risk

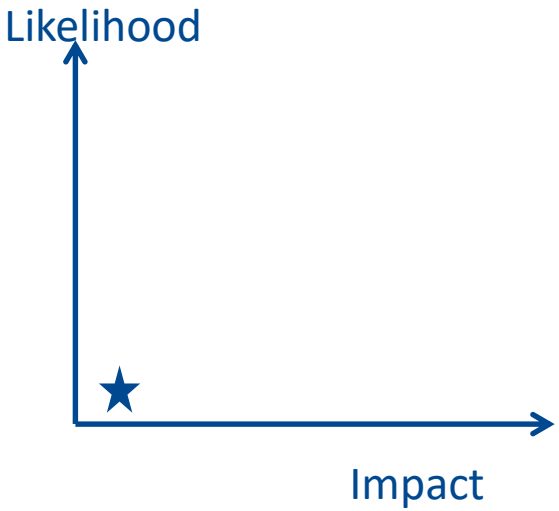


Technical Sources of Risk

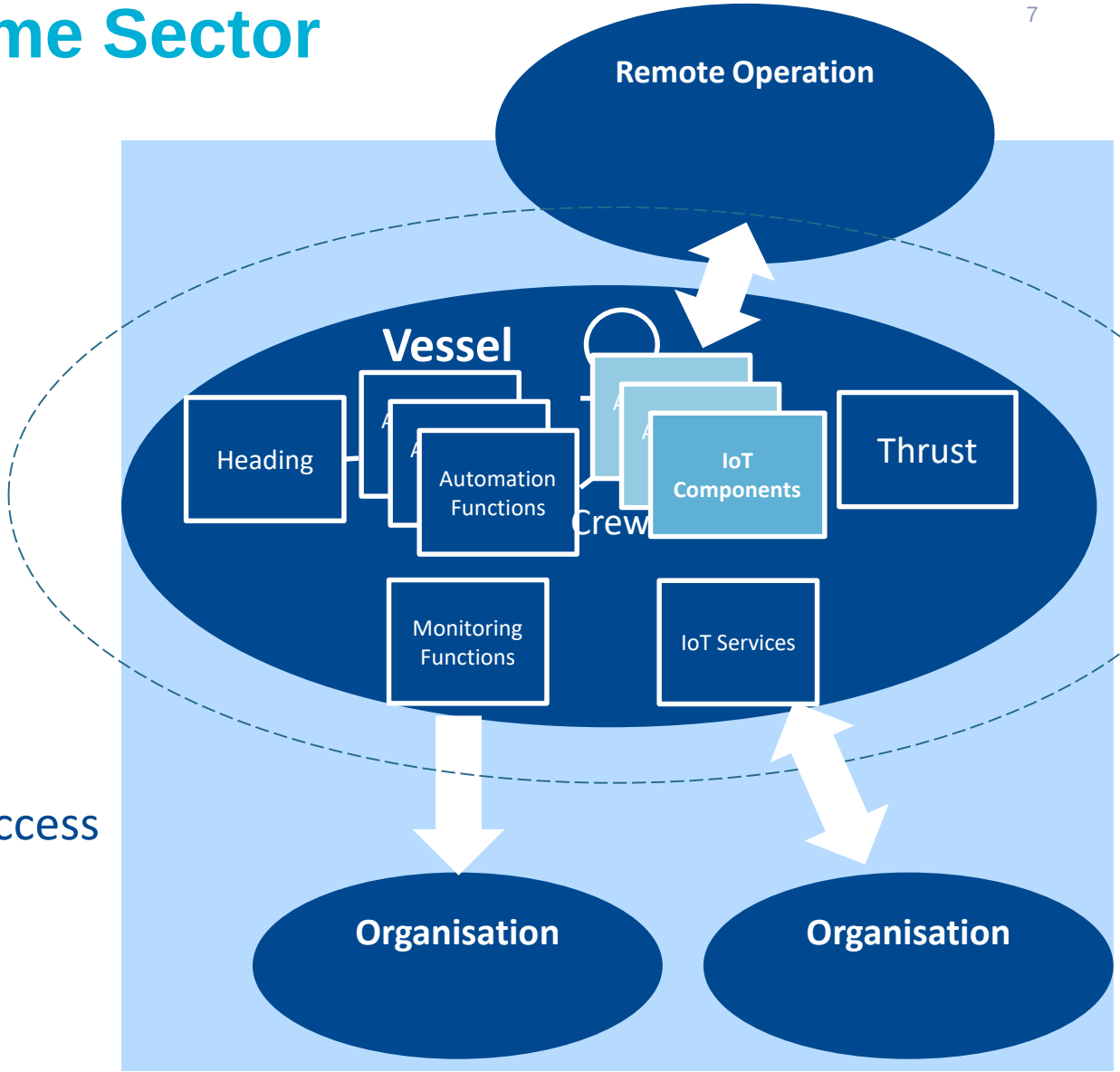


Rolls-Royce

Example: Maritime Sector



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



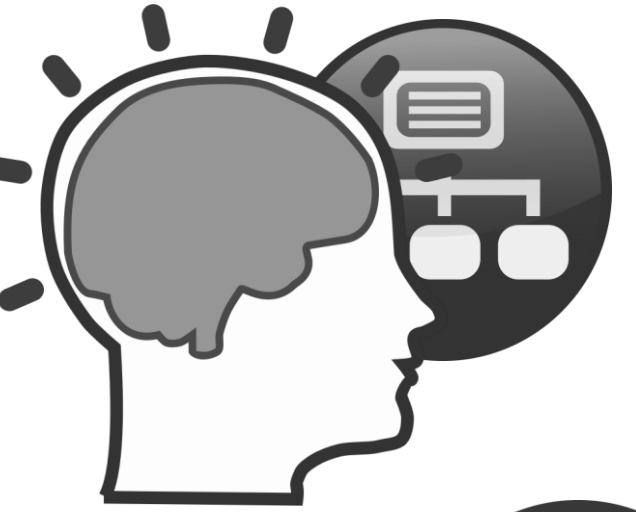
Rolls-Royce

Attacker Capability – Who is attacking?

CNI Attackers (From GAO)**:**

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

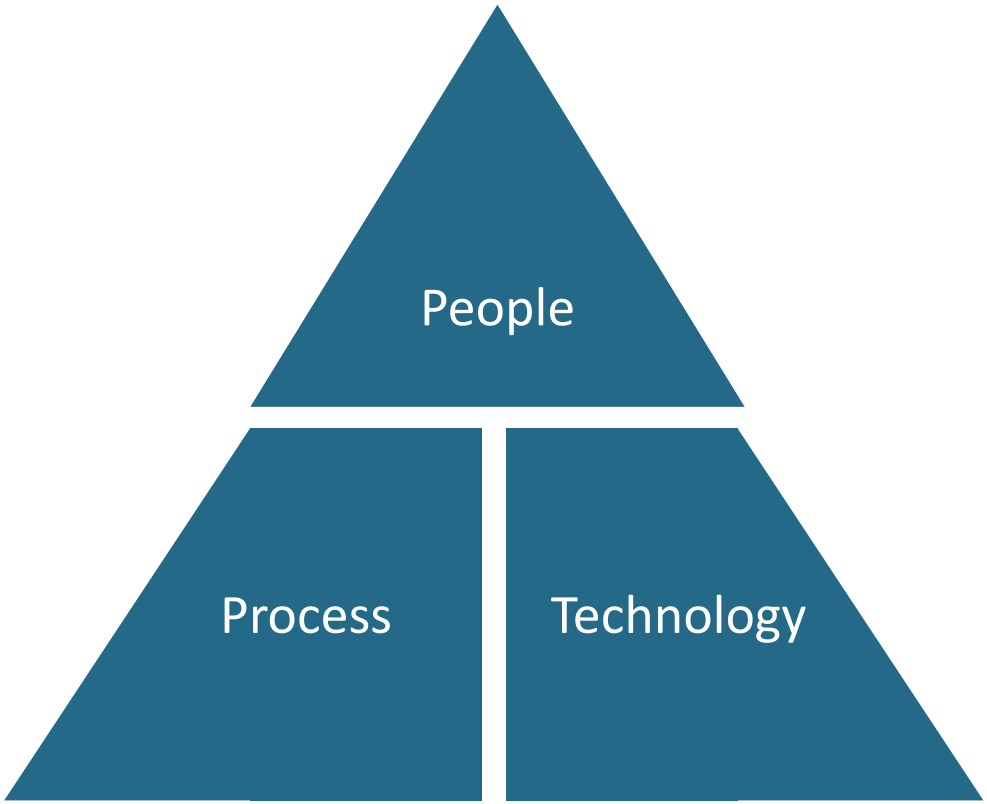
Attacker resources



Attacker Capability / Motivation

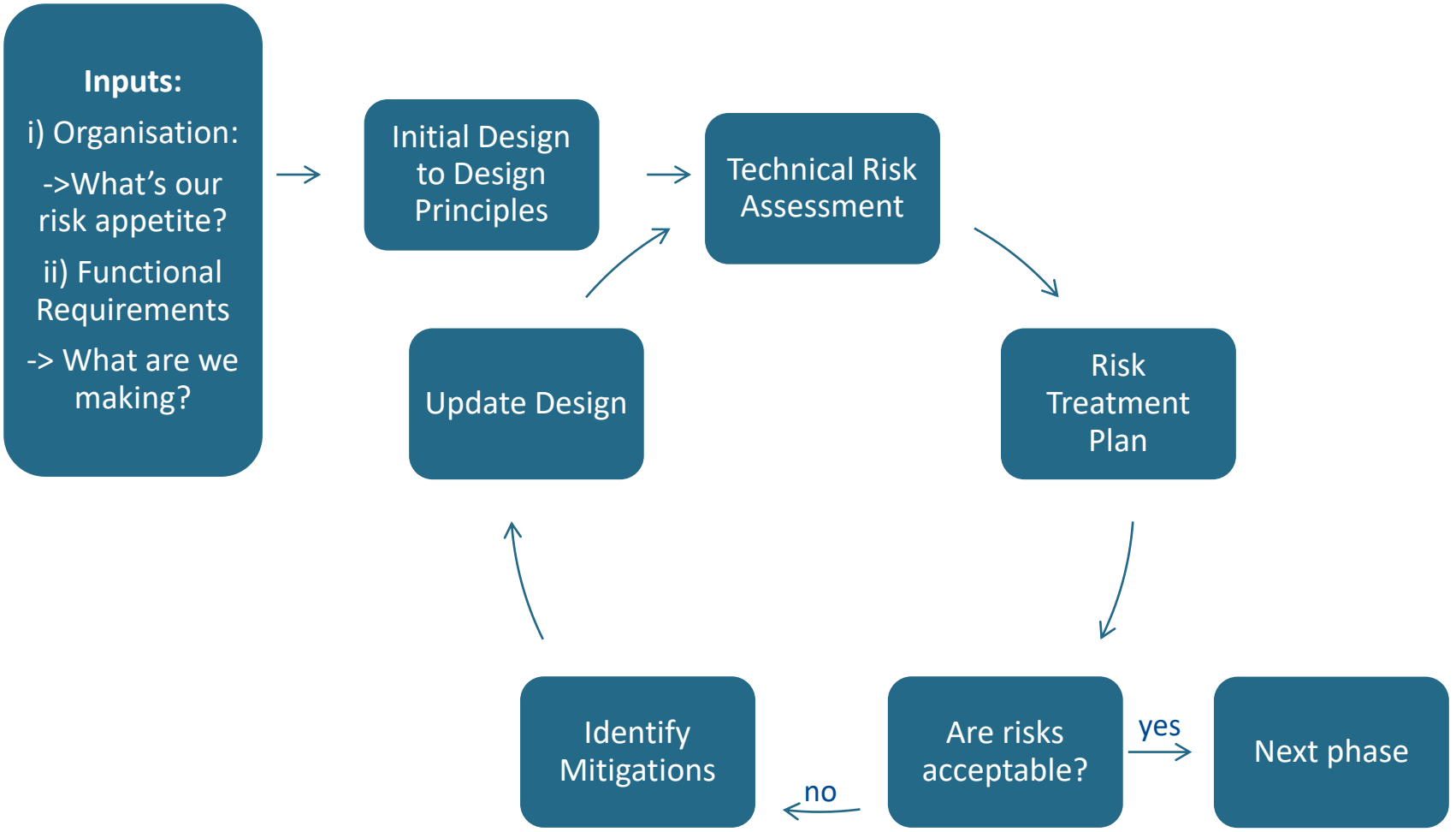
Rolls-Royce

What can we do about PCS Risk?



Rolls-Royce

Risk Driven Design Processes



Rolls-Royce

Secure Development Objectives

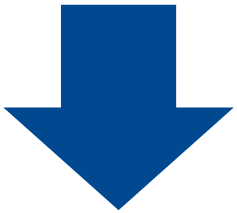
Security requirements across all sub systems to ensure that the system is secure at the system level

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

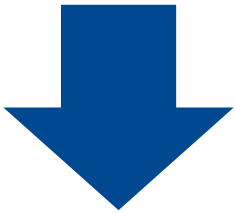
Security Champions

Communication

Rolls-Royce

Changing Cultures

Proportionate, risk-based controls



Keep costs down

Keep risks down

Understand risk

Rolls-Royce

Risk Sources

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

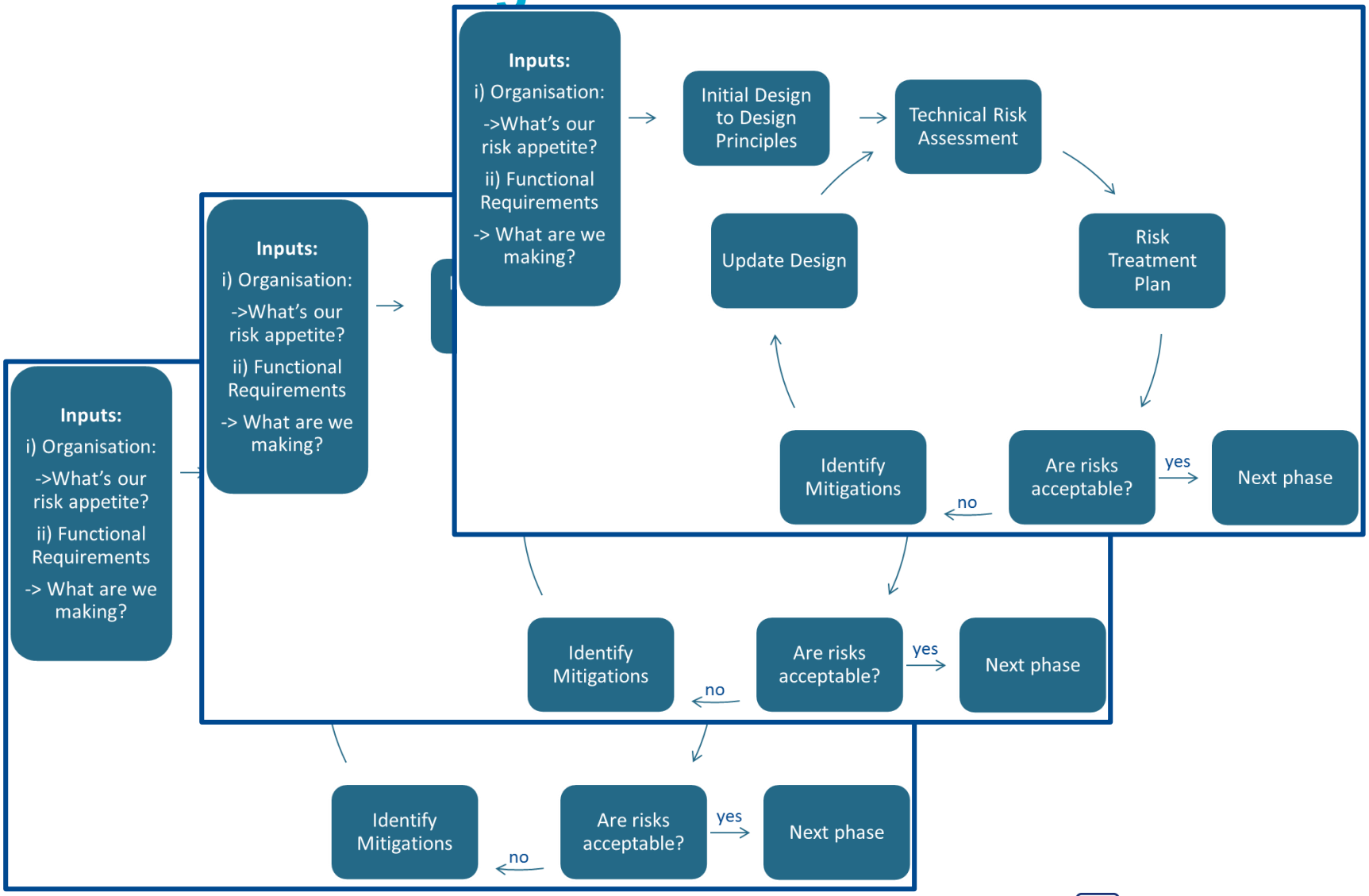
SAFETY

≠ SECURITY

CRYPTO

Rolls-Royce

Risk Driven Design Processes



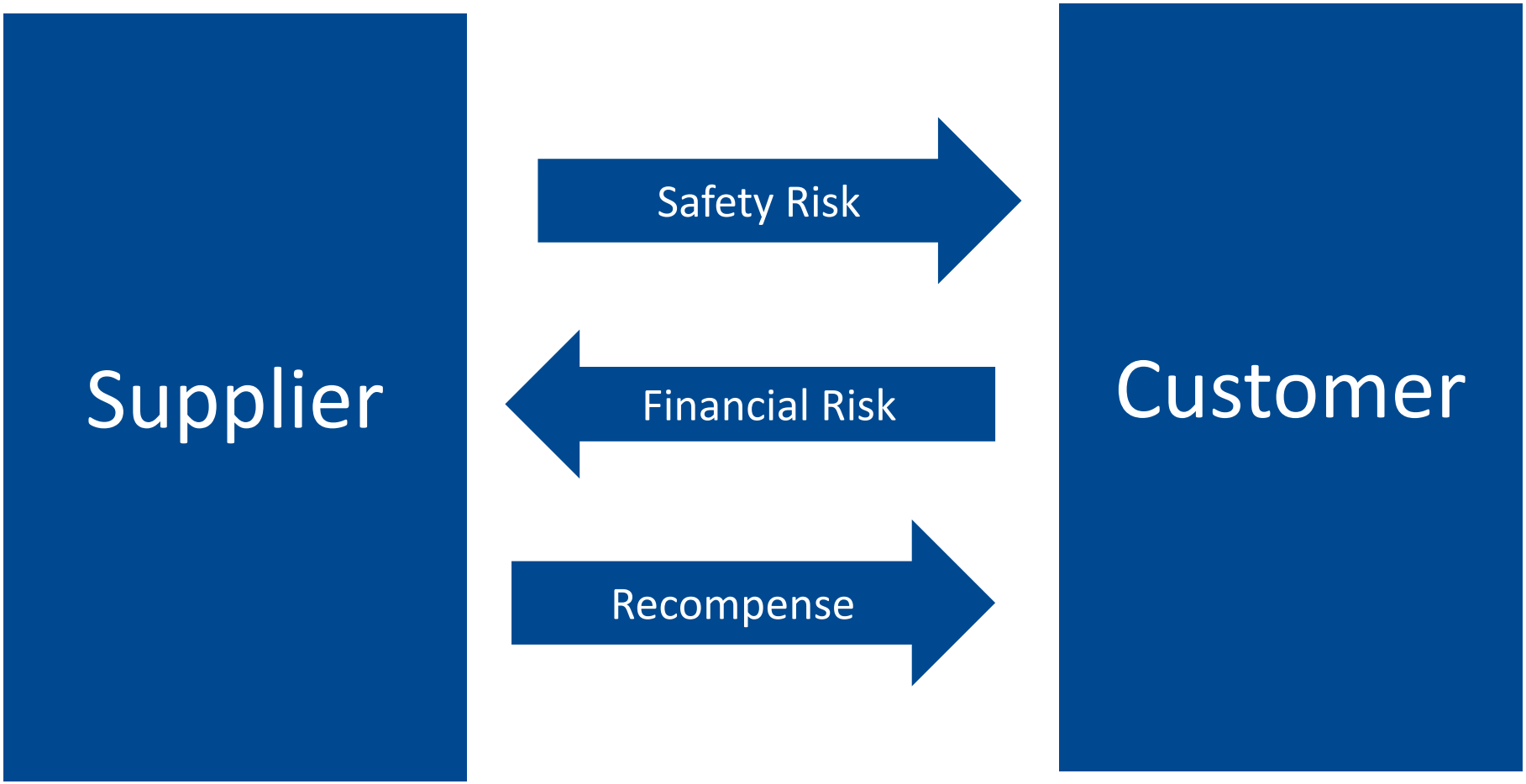
Rolls-Royce

Statement 2

Understanding the link to safety can make things

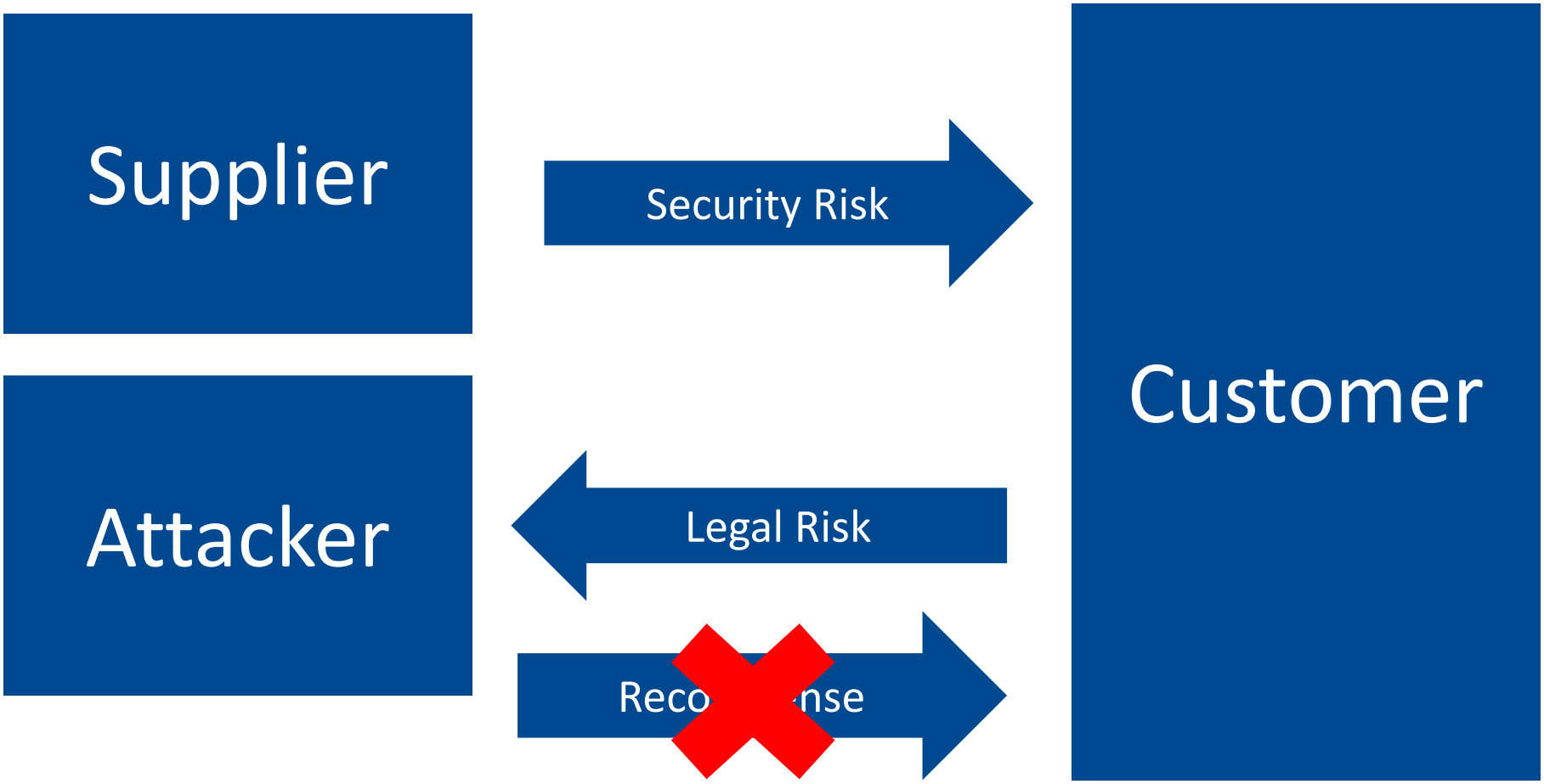
1. Safer
2. More secure
3. Cheaper

Risk Direction: Safety



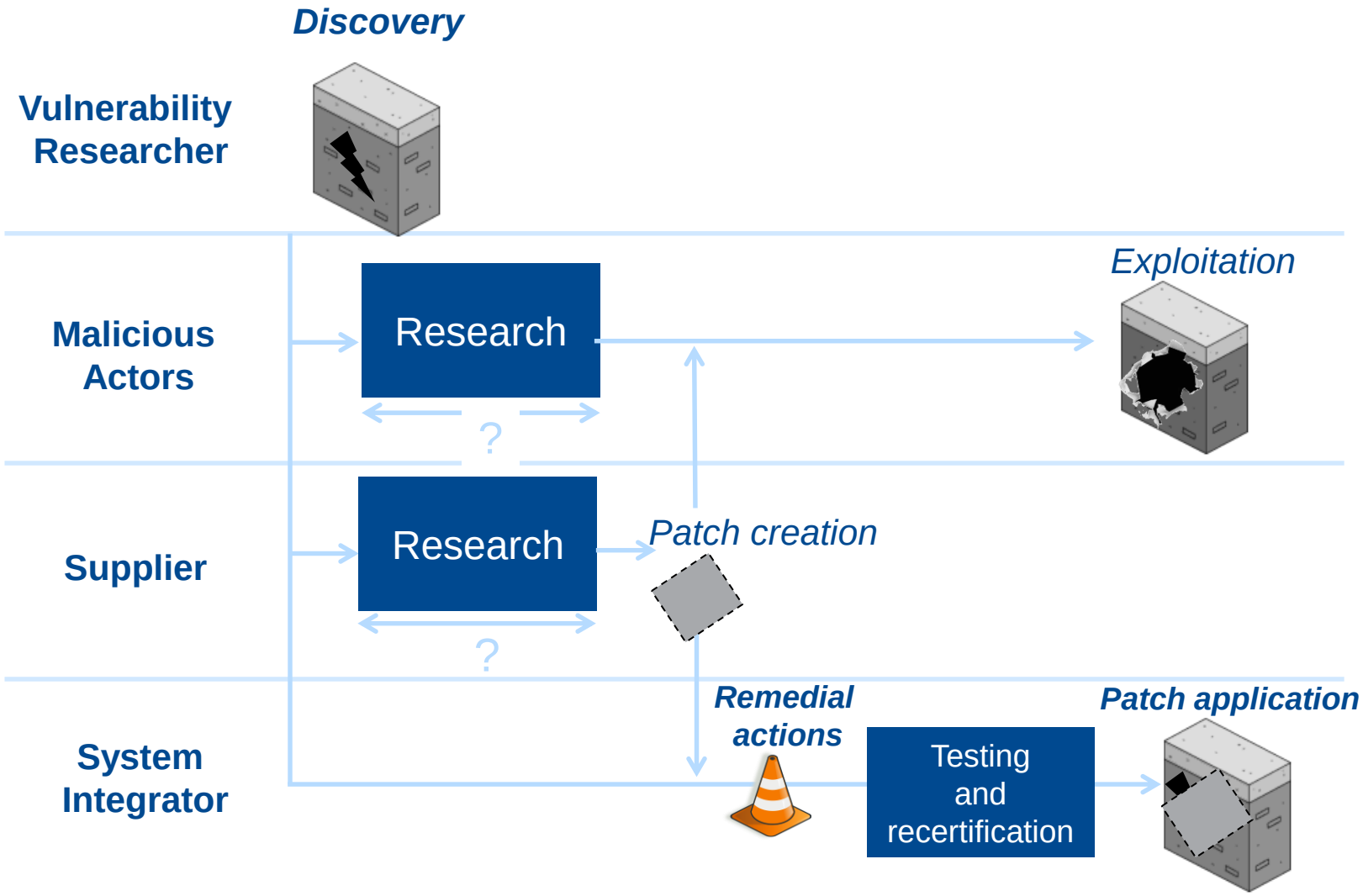
Rolls-Royce

Risk Direction: Security



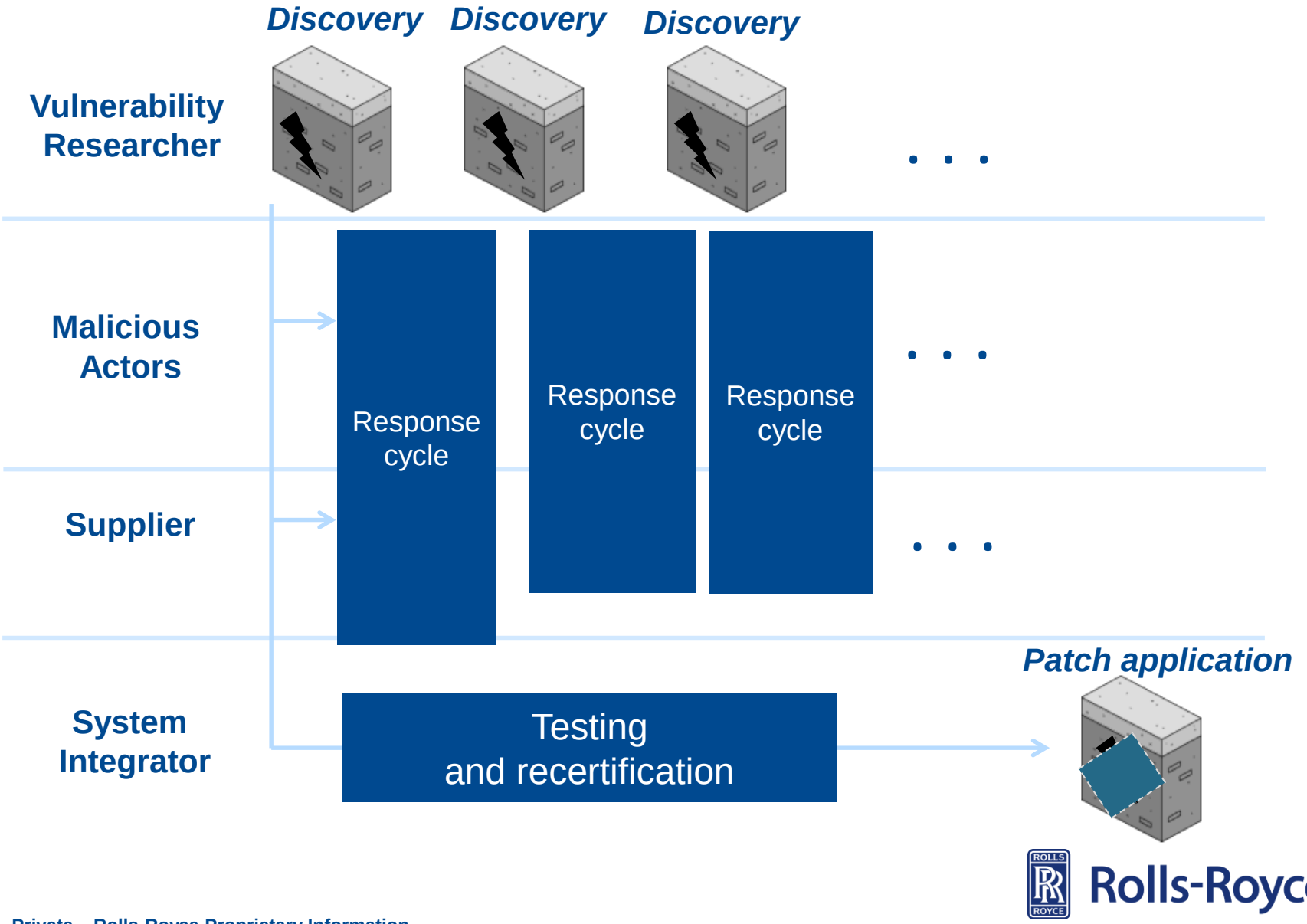
Rolls-Royce

Patching safety critical systems



Rolls-Royce

Patching safety critical systems



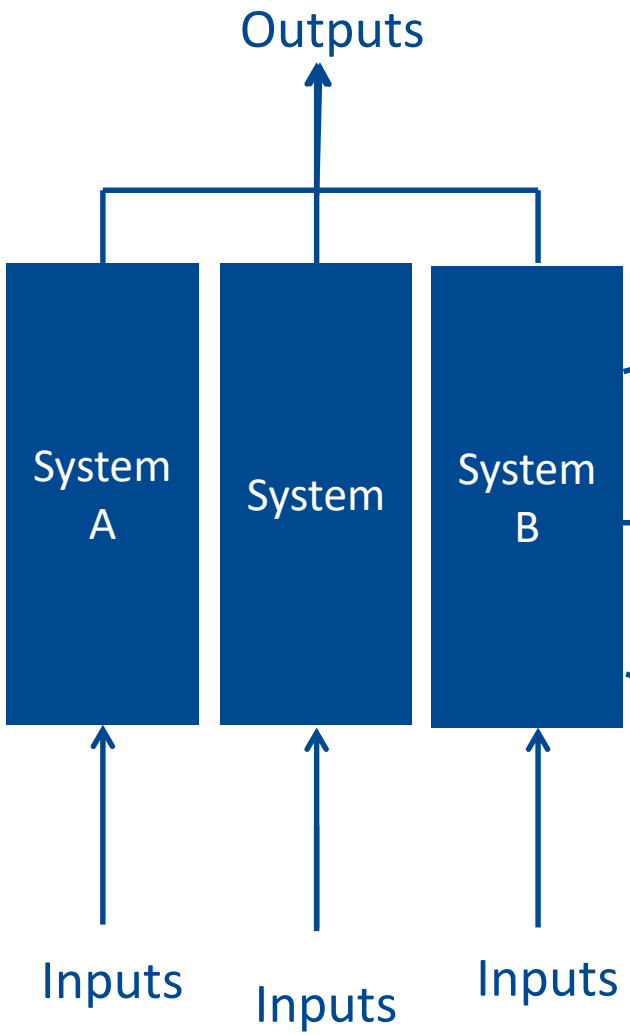
Design Principles in Opposition: Diversity

Safety

P(failure) = (0.0000001)^2

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

Extremely Low risk system



Security

Likelihood of attack?

Implementation specific vulnerabilities

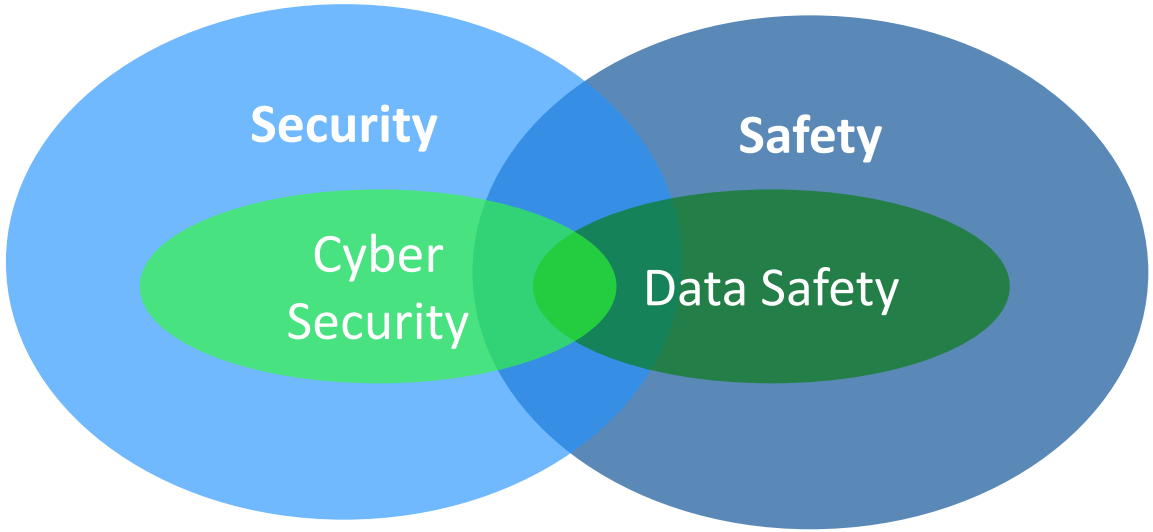
Specification vulnerabilities

Component vulnerabilities

Risky system!

Rolls-Royce

Understanding Risk



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

Technology

Resist	Detect and React
Network architecture • Interface control • Firewalls • Data diodes • Segregation Protocol Selection Cryptographic techniques • Cryptographic agility – quantum! • Legal issues Multi-source localisation Manual override	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/maintainance 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**