



The information in this document is proprietary and confidential to Rolls-Royce; and is available to authorised recipients only – copying and onward distribution is prohibited other than for the purpose for which it was made available.

Engineering Assets to be Safe and Secure

An Aerospace Perspective

Dr Robert Oates, Head of Product Cyber Security (Civil Aerospace)

© 2020 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.



US Revives Airplane Cybersecurity Bug Hunt

Tom Jowitt, October 1, 2019, 11:11 am

CYBERCRIME

SECURITY

SECURITY MANAGEMENT



Researcher S...
Flight Airplan...

IOActive researcher will
equipment can be 'we'

It's been four years r
world with his child
that could be abor
ships, military or

Santamarta h
level of terr
and satcor
research
devices

He a
and
w
f

plane

hangar

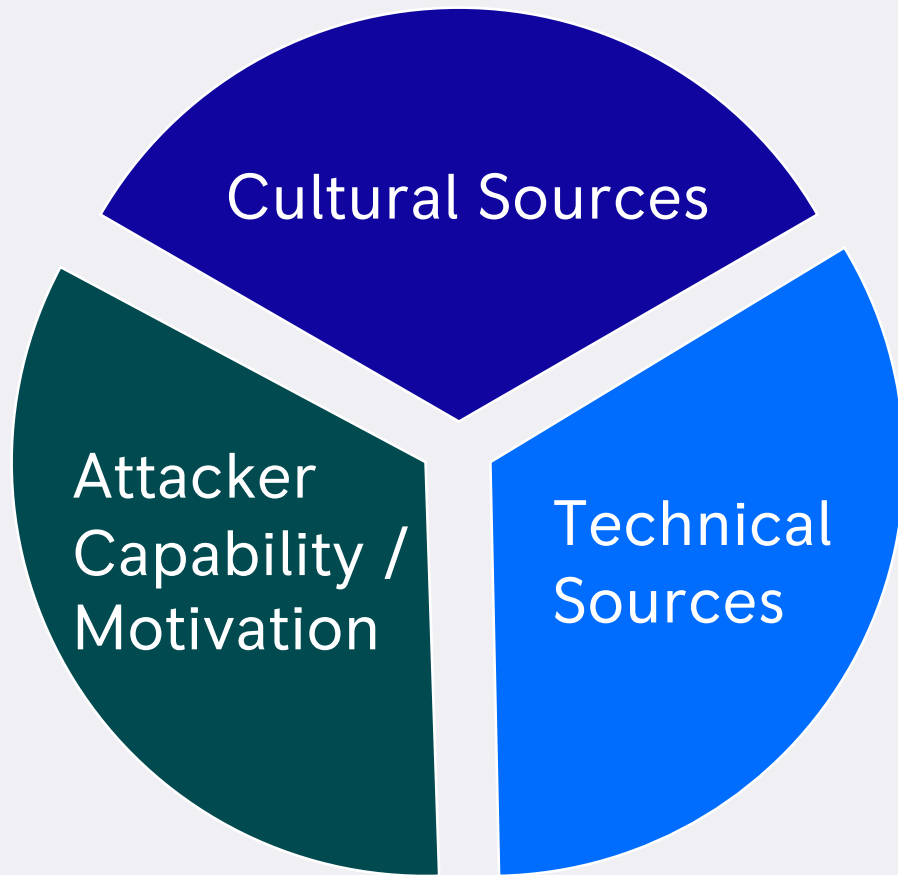
SHARE



er attack"



Sources of Risk Triplet





NIS-D

Legislative

Airworthiness

Safety /
Security
Assurance

Safety
Touchpoints

Incident
Response

Product
Design

Secure & Safe by design

Security Management
Plans

Safety Touchpoints for Cyber Security



Pearl 15 Engine



Rolls-Royce Swarm Robot Concept

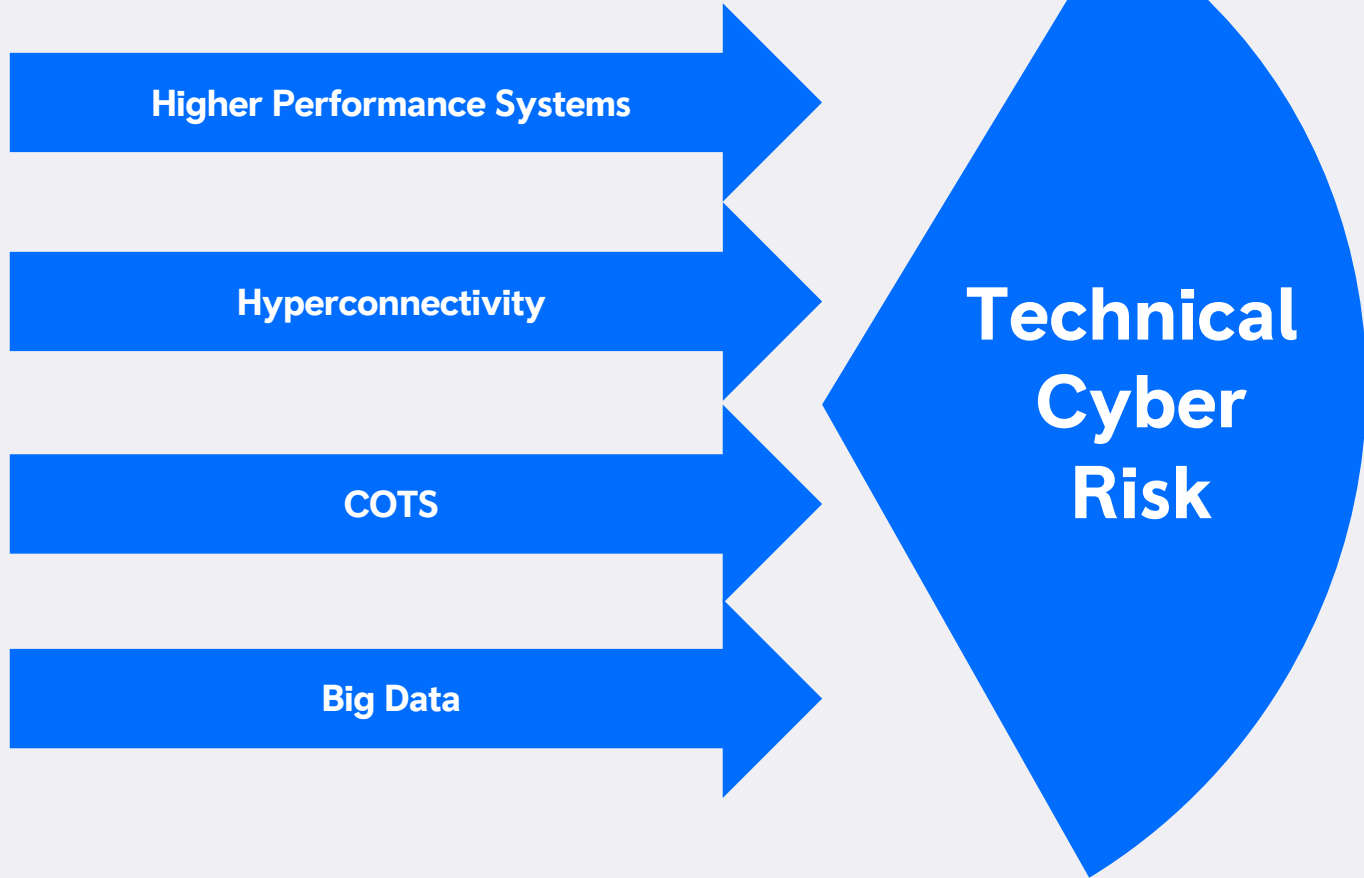


Rolls-Royce Personal EVTOL Concept



Technical Trends Across the Sectors

“Why are you
connecting *that* to
the internet!?”





Cultural Cyber Risk

Cultural Cyber Risk

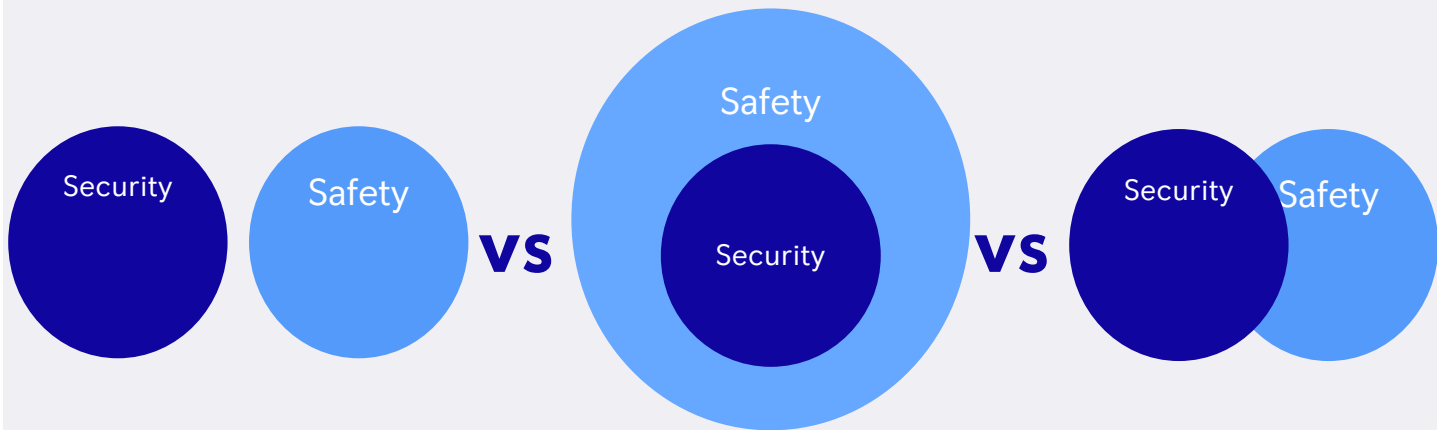
“If the hackers will get in no matter what we do what’s the point?”

“Isn’t this covered by IT / Safety?”

“This seems expensive!”

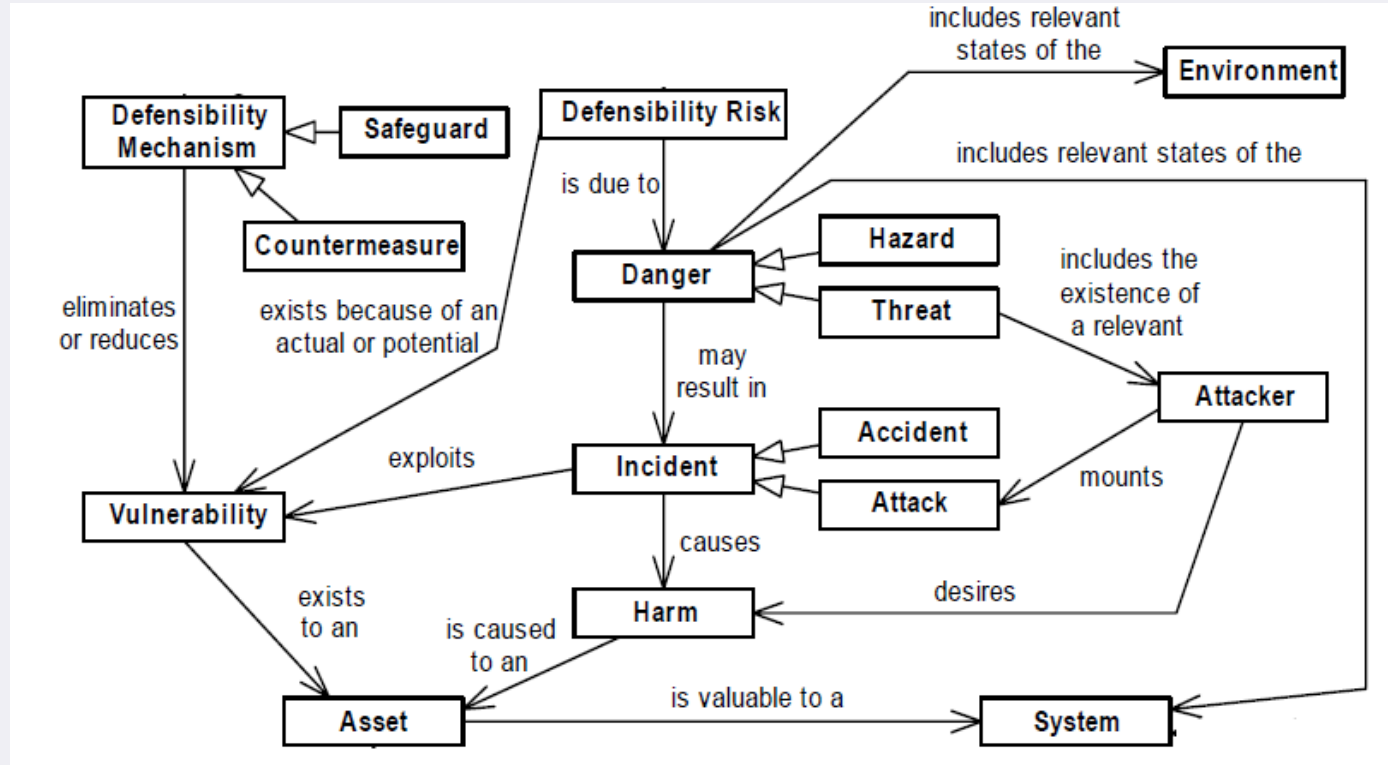


The Relationship Between Safety and Security



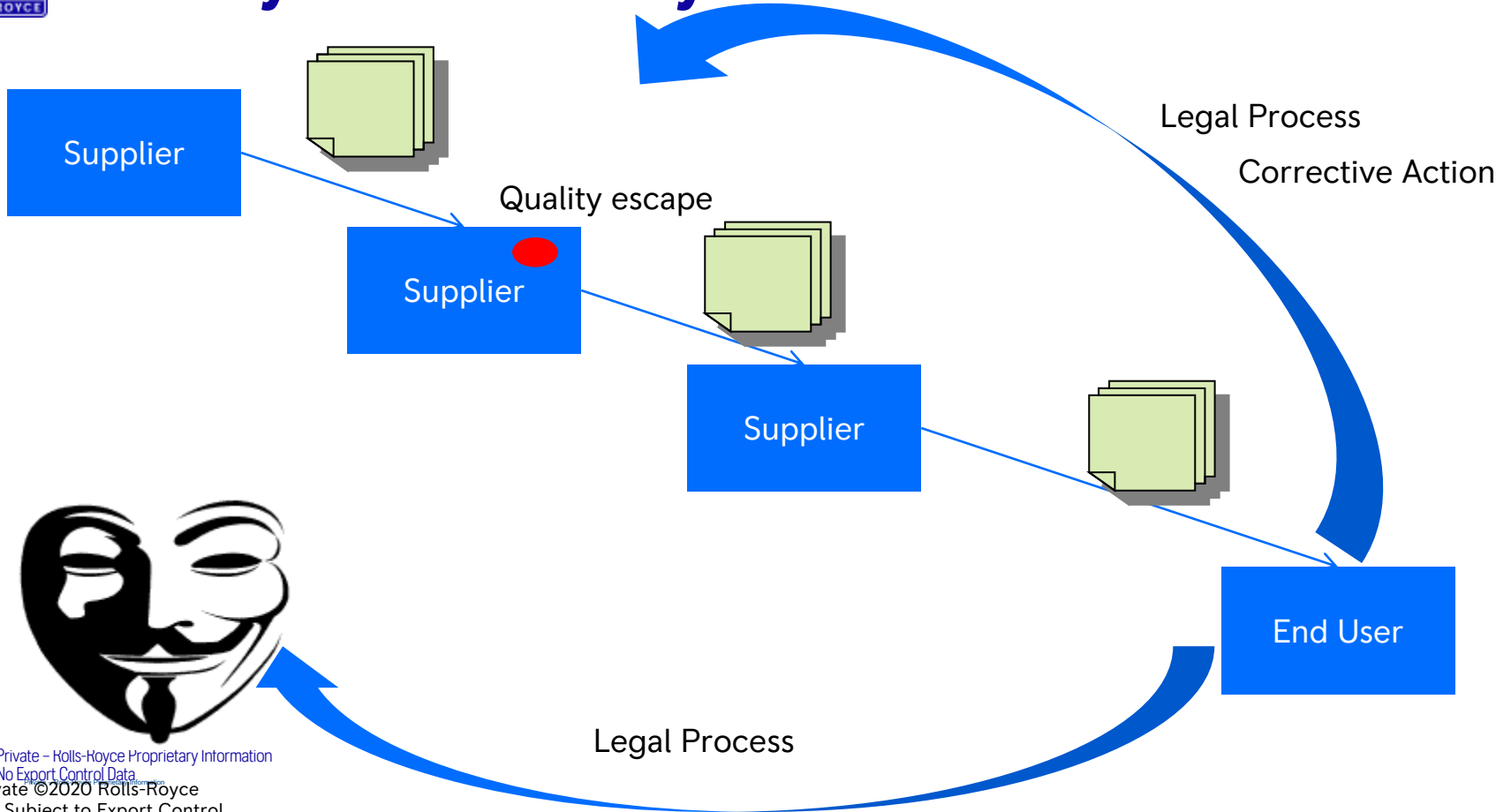


Firesmith Ontology Extract Firesmith 2005





Safety and Security - Risk



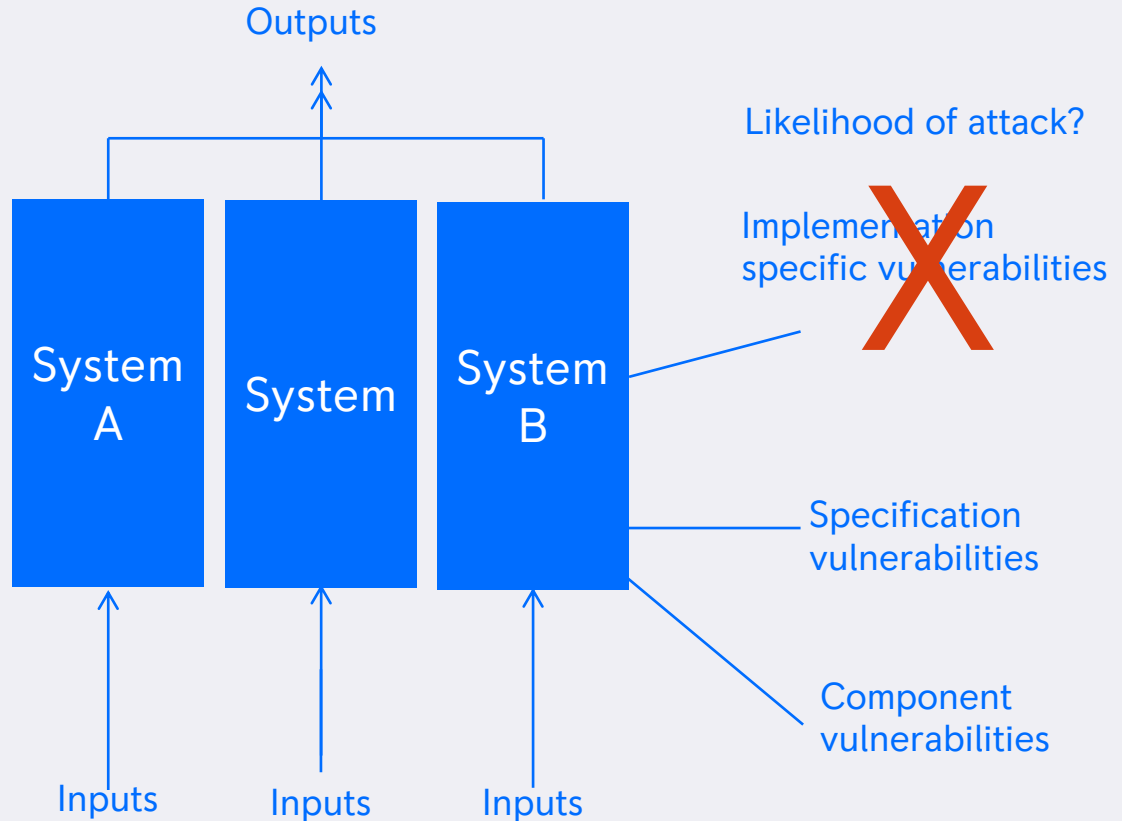


Safety

$$P(\text{failure}) = (0.000001)^2$$

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

Security



Extremely Low-risk system

Design Principles in Opposition: Diversity

Risky system!



Safety

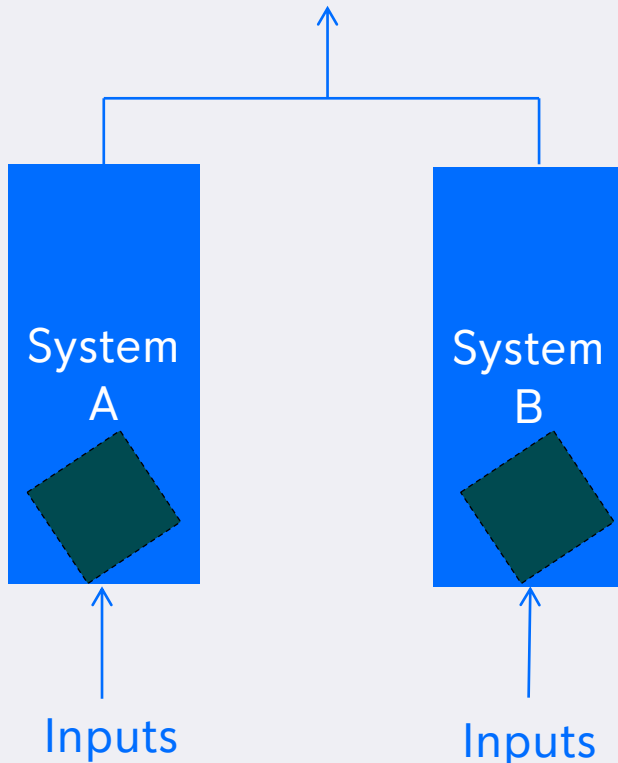
$$P(\text{failure}) = (0.0001)^2$$

Uncertainty: High! What has the patch done to our systems?

Need to retest, recertify....

Low Risk system

Outputs



Security

Likelihood of attack?

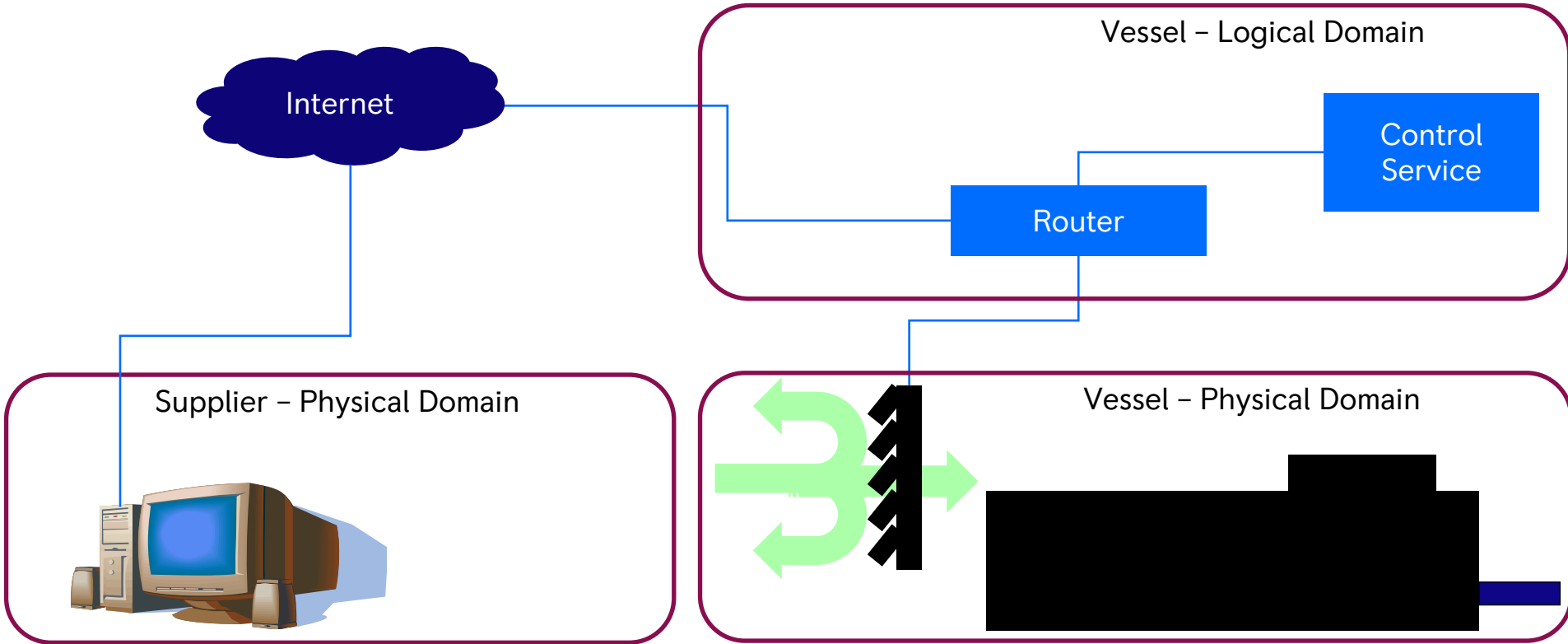
Vulnerability Report

Low Risk system?

Patching

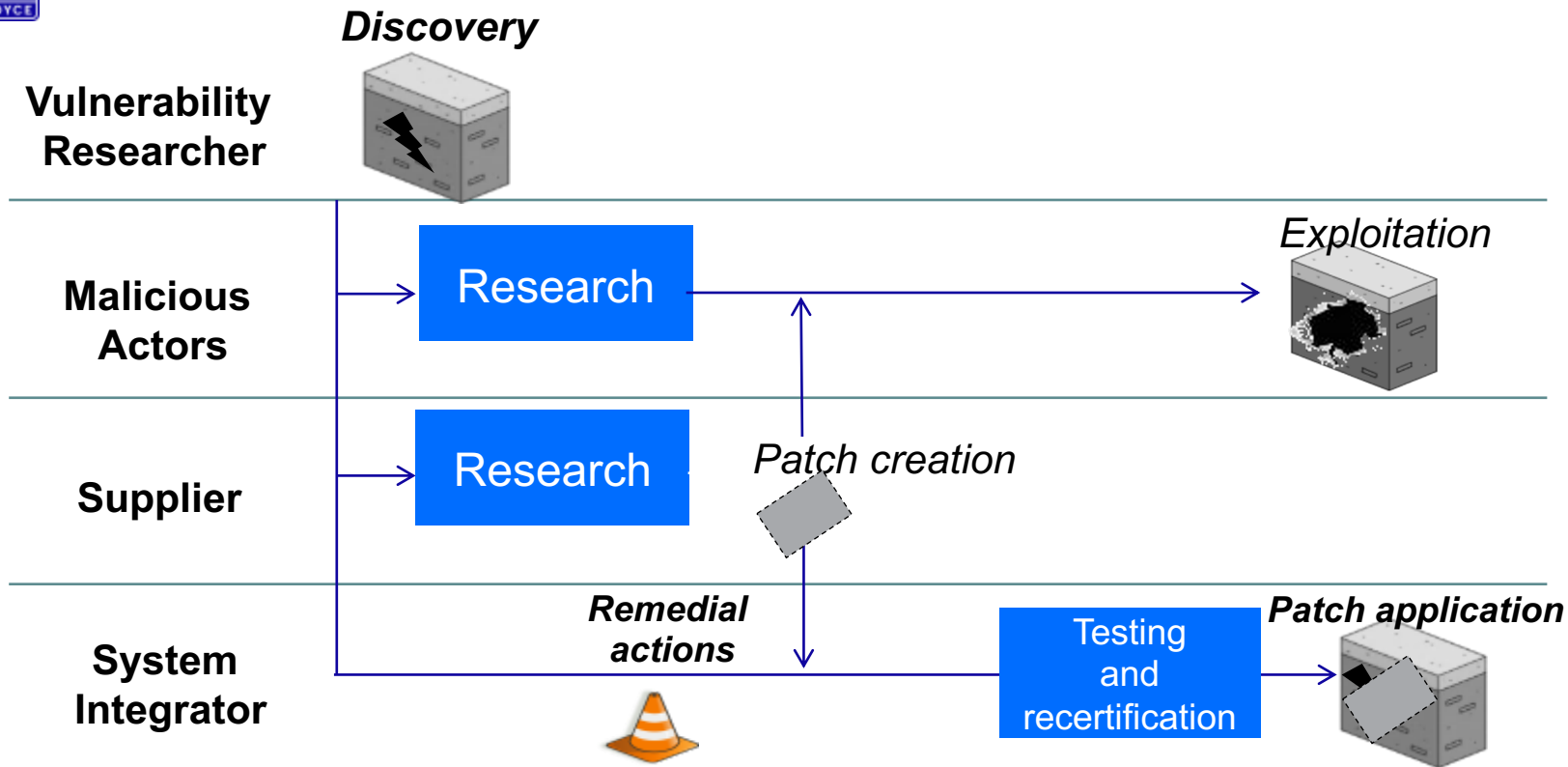


Case Study: Patching at Sea





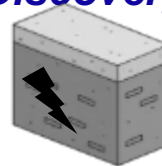
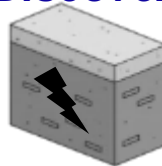
Patching safety critical systems





Patching safety critical systems

Discovery *Discovery* *Discovery*

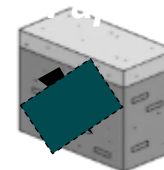


Response
cycle

Response
cycle

Response
cycle

Testing
and recertification





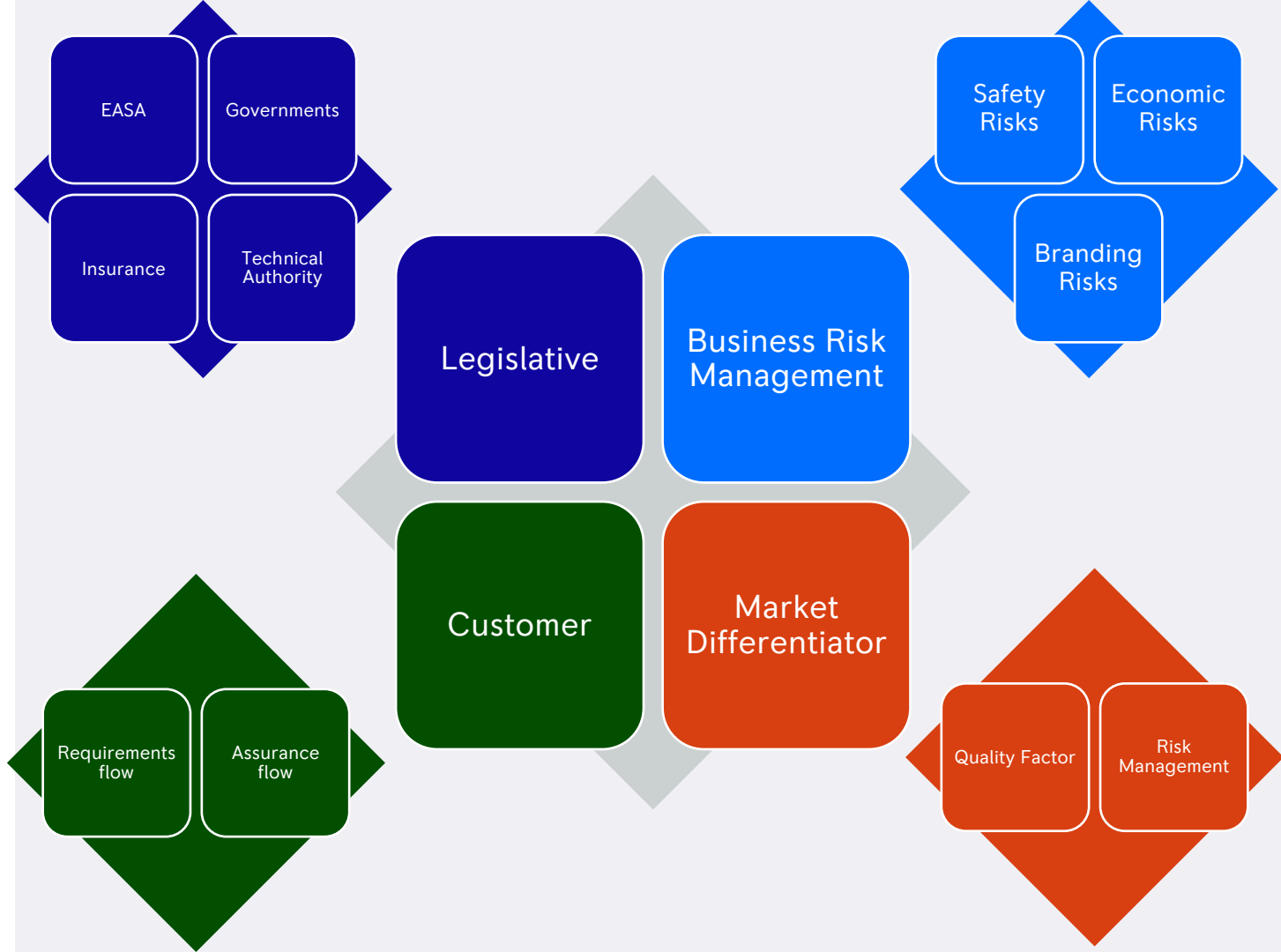
Attacker Capability and Motivation



**Attacker
Capability
/
Motivation**



Motivators for product cyber security





A Brief Introduction to Civil Aerospace Legislation



NPA 2019-01

NPA 2019-07

ED202A / DO-326A – Airworthiness
Security Process Specification

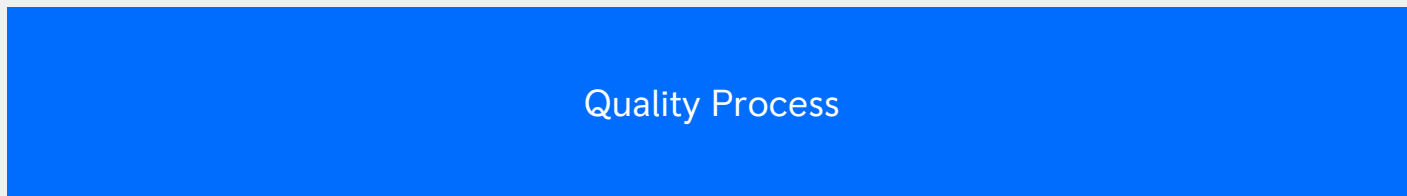
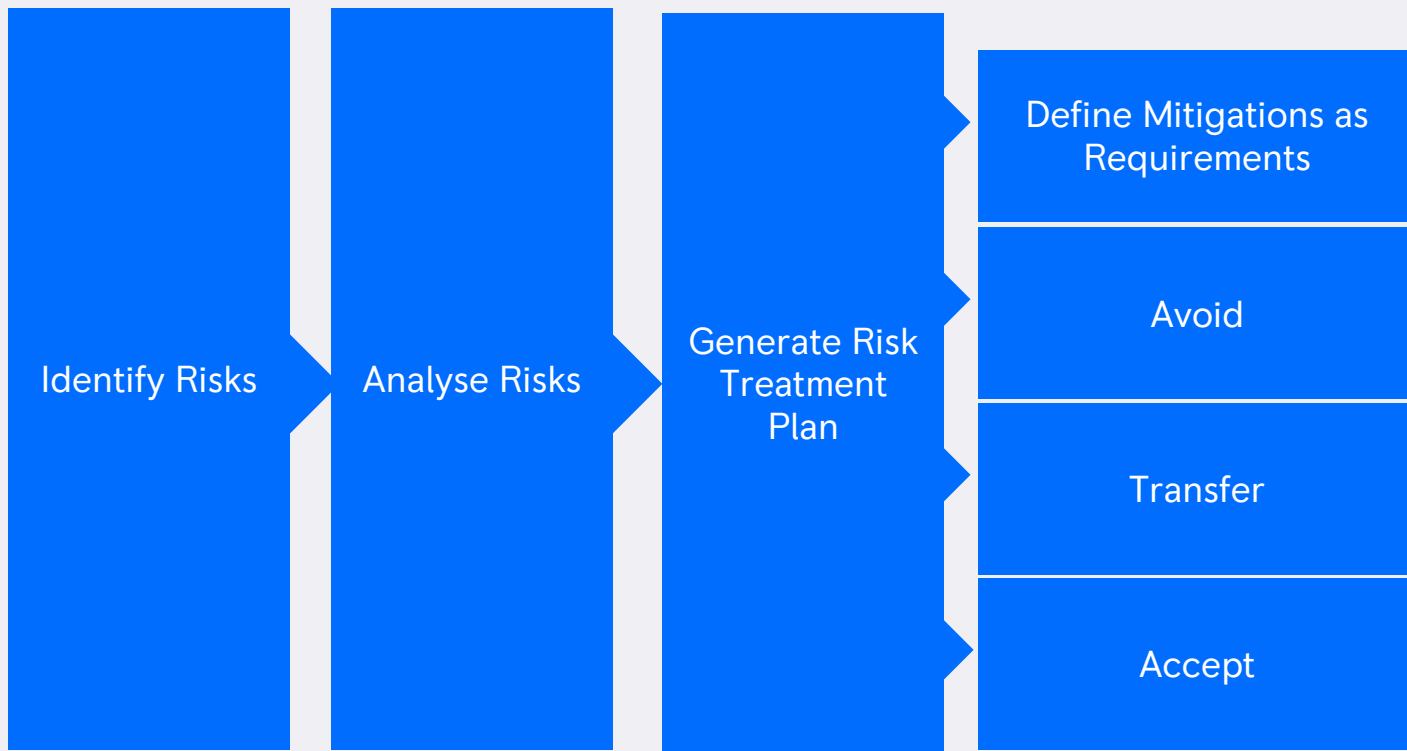
ED203A / DO-356A – Airworthiness
Security Methods and
Considerations

ED204A / DO-355A – Information
Security Guidance for Continuing
Airworthiness

Civil Aerospace Guidance



Risk Driven Development





Cyber Risk Management for Engineering

Functional Requirements

Systems Engineering Process



How do we identify/analyse the risk?

The Technical Risk Assessment Process

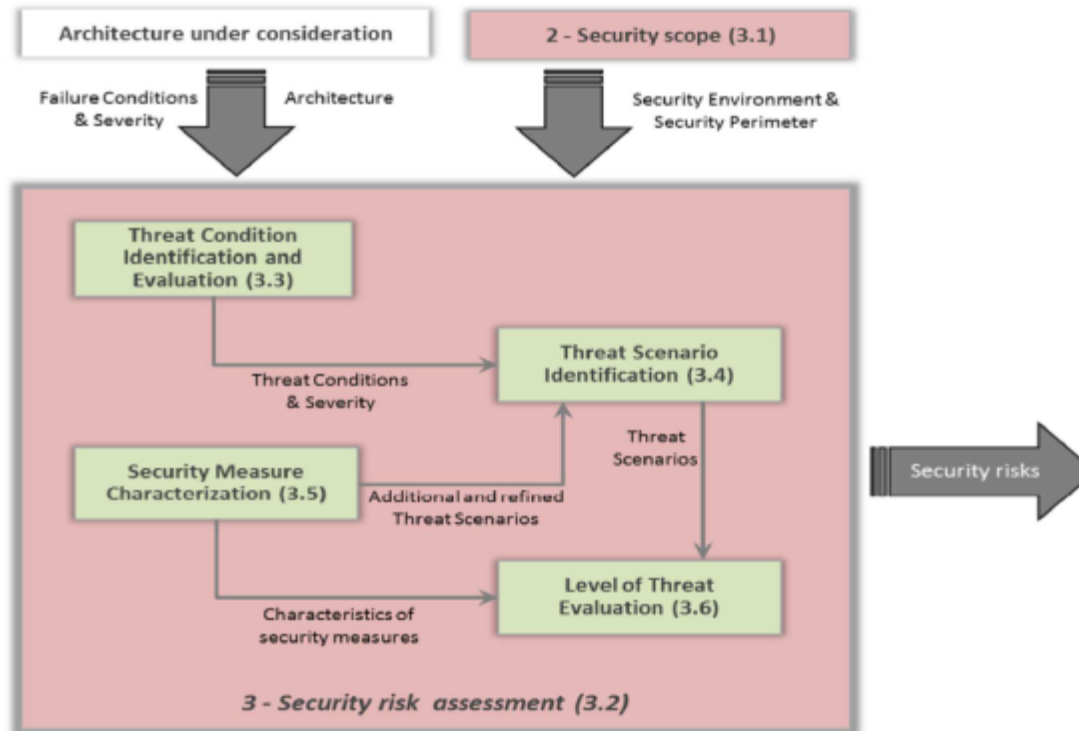
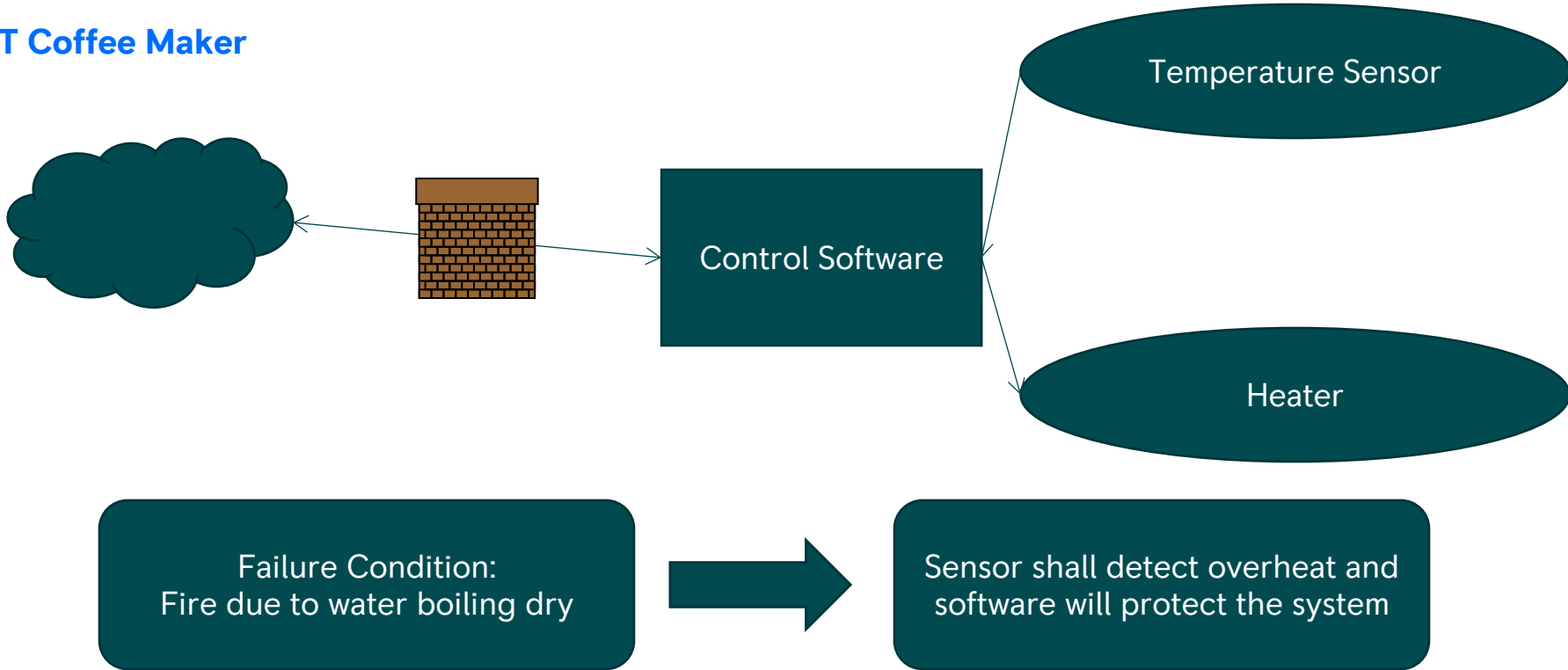


FIGURE 3-2: SECURITY RISK ASSESSMENT



IoT Coffee Maker



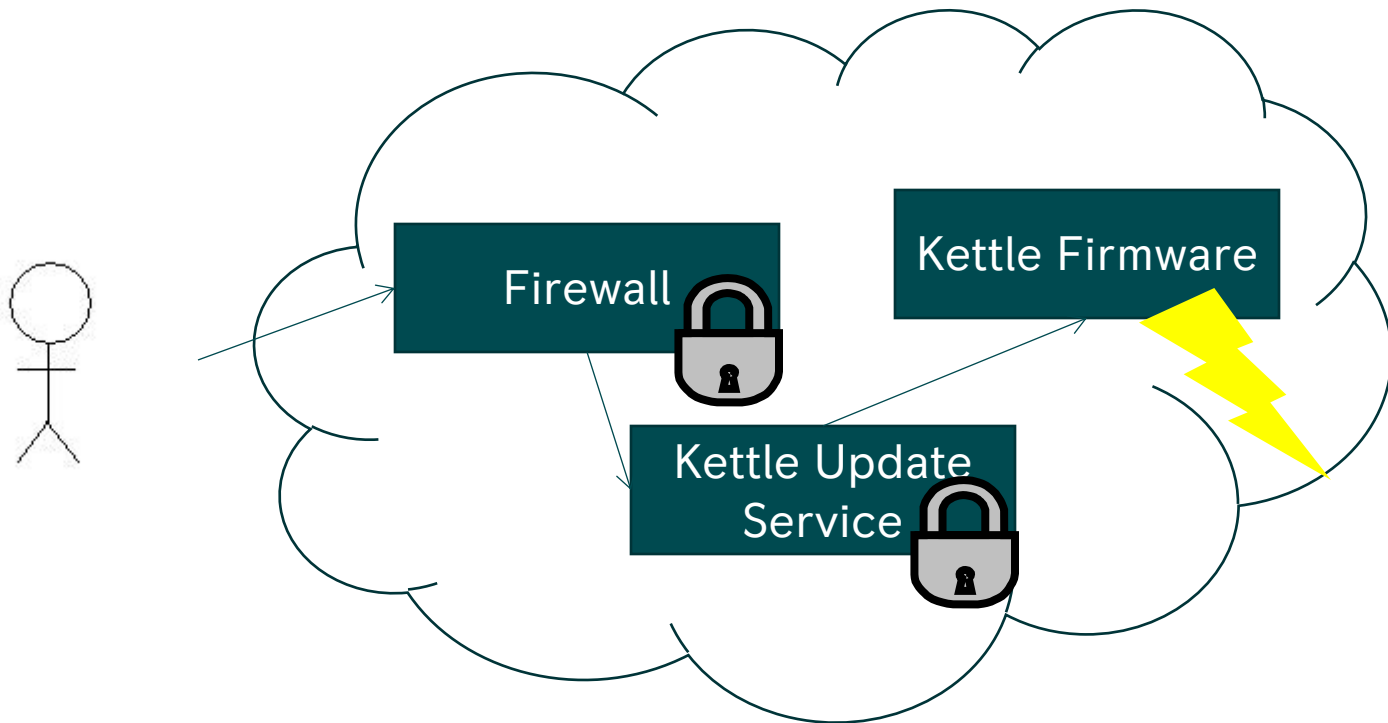
Failure Condition:
Fire due to water boiling dry

Sensor shall detect overheat and
software will protect the system



IoT Coffee Maker

Threat scenario: Attacker changes calibration data for sensor to cause fire





IoT Coffee Maker

1. Estimate Likelihood of attack launch
2. Estimate Likelihood of attack success
3. Estimate effectiveness of firewall as a control
4. Estimate effectiveness of update service as a control
5. Estimate overall effectiveness of controls and compare to risk



Conclusions

- Organisations are motivated to manage cyber risk and are doing so
- The legislative, risk, and technology landscapes are fast-moving
- The lifetimes of the products are very long
- The security process requires a lot of engineering judgement



Questions?