LEONARDO

Leonardo Cyber & Security Solutions

Assessing Cyber Security Risk associated with Mission Critical Communications over Public Networks

BAPCO 2023

Newcastle

15/11/2023

Electronics

Helicopters

Aircraft

Cyber & Security

Space

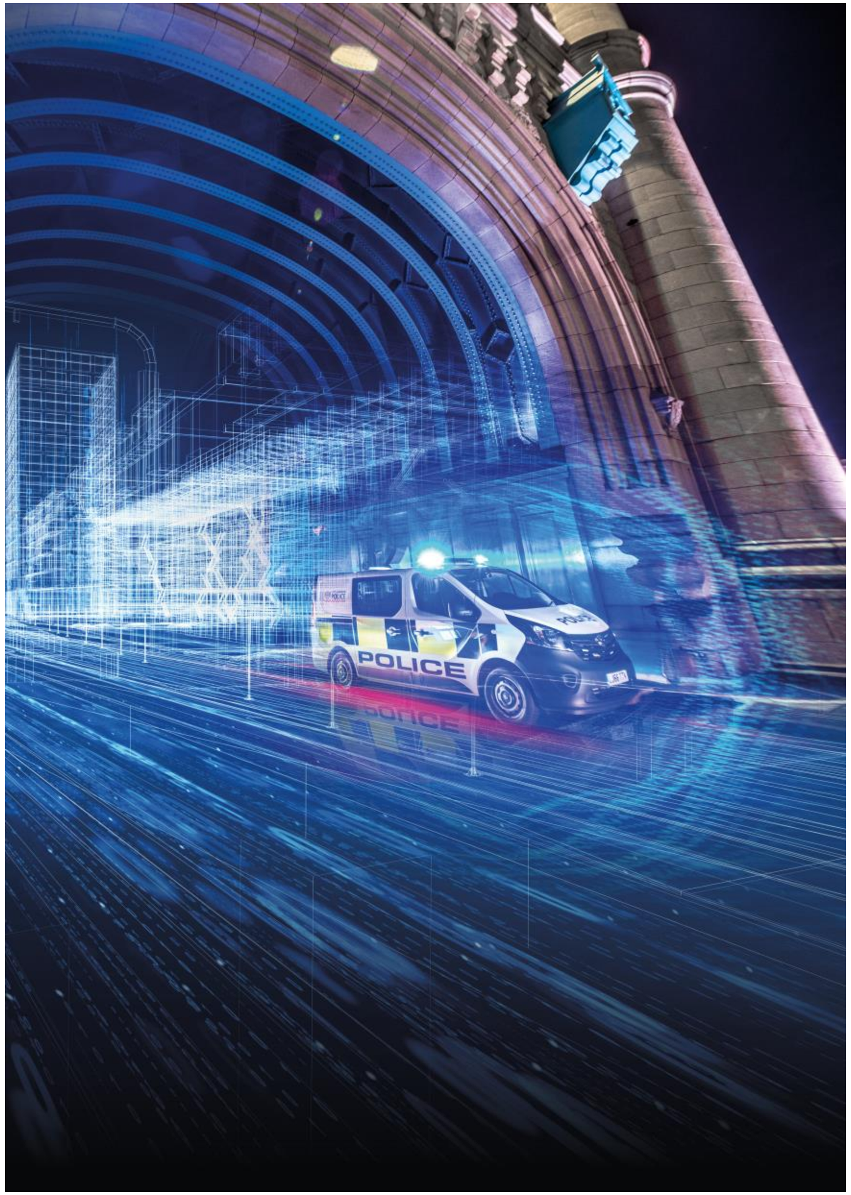
Uncrewed Systems

Aerostructures

Introduction & Objective

Setting the Stage

- Who am I?
- Who are you?
- Workshop: Consider points, apply context
- Speak to us



SUMMARY

- What is Cyber Security Risk?
- What are the system properties we are striving to protect?
- What threats are we facing?
- How do we approach protecting our system?
- What are the key challenges in our context?
- Questions

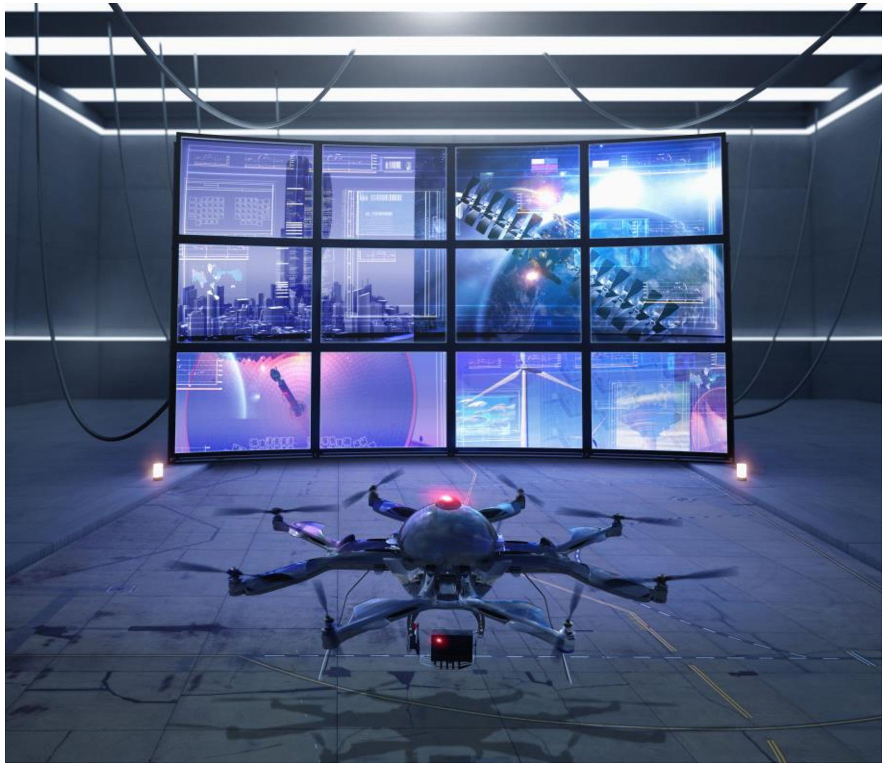
What is Cyber Security Risk?

Identifying the components of risk

What is Cyber Security Risk?

Describing Risk

- A risk is the **likelihood** that a **threat** will exploit a **vulnerability** resulting in an **impact**.



What is Cyber Security Risk?

Risk Components

- Threat – an intentional, reckless or accidental entity
- Adversarial, Non-Adversarial
- Vulnerability – a weakness
- Exposure amplifies vulnerability
- Likelihood – chance or probability
- Impact – consequence
- Impact & Likelihood can be expressed either quantatively or qualitatively
- Risk level is derived from a function of Impact & Likelihood
- Risk must be treated – Accept, Avoid, Reduce, Transfer

What properties are we trying to protect?

The 3 Pillars of Information Security

What properties are we trying to protect?

The 3 Pillars of Information Security

- CONFIDENTIALITY
- INTEGRITY
- AVAILABILITY

What properties are we trying to protect?

The 3 Pillars of Information Security

- Confidentiality – restricting access to information to those with a need to know
- Integrity – restricting operations on information to those with necessary privilege
- “Least Privilege”
- Availability – maintaining information and operations in a usable state

What threats are we facing?

The two categories of Threat

What threats are we facing?

The 2 categories of threat

- ADVERSARIAL
- NON-ADVERSARIAL

What threats are we facing?

The 2 categories of Threat

- Adversarial – likely to be linked to context
- Nation State, OCG, Competitor, Hacktivist, Insider, Script Kiddie
- Non-Adversarial – typically Users & Environments

How do we approach protecting our system?

Supporting the 3 pillars of Information Security

How do we approach protecting our system?

Supporting the 3 Pillars of Information Security

- C – AUTHENTICATION; ACCESS CONTROL; ENCRYPTION
- I - PRIVILEGE MANAGEMENT; ERROR DETECTION & CORRECTION
- A - RESILIENCE, REDUNDANCY & RECOVERY

How do we approach protecting our system?

Supporting the 3 Pillars of Information Security

- Mutual Authentication, Access Control & Privilege Management - a fusion of Governance & Technology

- Encryption, Error Detection & Correction delivered through Industry Standards

- High Availability – Network Dependent

What are the key challenges in our context?

Common Risks in a Critical Communications context

What are the key challenges in our context?

Prioritisation in the context of Mission Critical Communications

- CONFIDENTIALITY – **may** impact the mission
- INTEGRITY – **may** impact the mission
- AVAILABILITY – **will** impact the mission

What are the key challenges in our context?

Identifying core threat

- In most contexts, the greatest threat is likely to be **non-adversarial**

- Controversial or accurate?

What are the key challenges in our context?

Addressing Challenges – Confidentiality & Integrity

- C/I is likely delivered via industry standards
- Vulnerability through poor implementation

- Backward Compatibility
- Exposure at End Points

- Secure by Design
- Compliance, Assurance and Testing
- Security Updates/Asset Management
- Detection and Response

What are the key challenges in our context?

Addressing Challenges – Availability

- Highly situational
- Extreme Environments

- Coverage
- Call Prioritisation

- End User informed
- Recent & Comprehensive Experiences
- Threat Modelling & Continual Coverage Test
- Response & Recovery Exercising – Continuous Improvement

QUESTIONS

CONTACTS

Leonardo Cyber & Security Solutions

Dan Maund

Managing Consultant

Daniel.Maund@Leonardo.com

LEONARDO

THANK **YOU**
FOR YOUR ATTENTION

uk.leonardo.com