cds Defence & Security

DEFENCE EQUIPMENT SAFETY

THE CYBER DIMENSION

CAN DEFENCE EQUIPMENT EVER TRULY BE CONSIDERED SAFE WITHOUT INCORPORATING CYBER SECURITY?

01: IMAGINE THE SCENARIO

A medium size helicopter with 12 crew on board is on exercise in Afghanistan and returning to base. The operational flight is being carried out in limited visibility (Instrument Meteorological Conditions (IMC)) so the crew is operating on instruments alone.

During the concept stage of the build of this aircraft, three companies were involved in the component software development. During meetings, many notes were taken and instructions written up. As these documents were official sensitive, and therefore housed on unprotected systems, they were able to be accessed by a number of people in the company.

Enemy insurgents have been sold these documents and, during the flight back to base, they are able to disable the Terrain Avoidance System (TAS). Loss of the TAS causes reduction in crew situational awareness and the aircraft flies into the mountain (controlled flight into terrain) resulting in loss of the aircraft and the death of all 12 crew onboard.

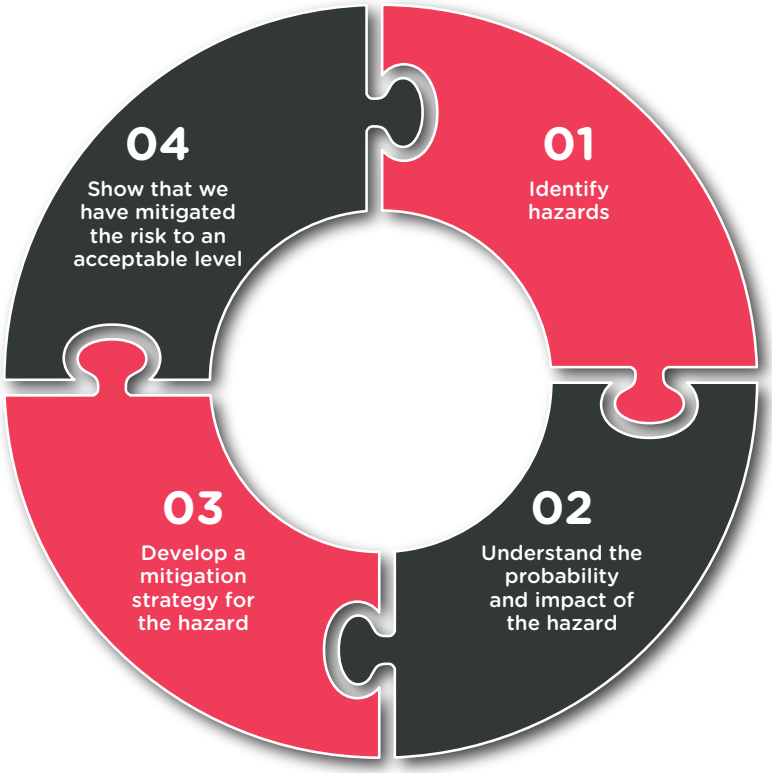
02: THE SAFETY APPROACH

Now, while this scenario hasn't happened yet, the fact that a third party being able to hack into the software wasn't considered during the safety assessment shows just how little cyber security is planned for in the design and build of defence programmes.

At present, the high-level view of safety is around preventing accidents and reducing the risk to life. We understand the route to an accident via causes and hazards for example, a lack of training or a process not being followed properly. We then impose standards to ensure these hazards are mitigated.

Safety forms part of the CADMID (Concept, Assessment, Development, Manufacturing, In-Service, Disposal) process of equipment acquisition.

During the concept stage, we establish a strategic approach using common systems such as POSMS (Project Oriented Safety Management System). We then develop a plan, most commonly a Safety Environment Management Plan (SEMP) which enables us to manage the process.



THIS IS THE POINT WHERE WE SHOULD BE ASKING THE FOLLOWING QUESTIONS:

In the scenario we referenced earlier, the answer to most of these questions was quite clearly, yes, So why are we not considering the impact of cyber security breaches or compromises in relation to equipment safety?

01 Does the lack of effective cyber security (controls) create any additional hazards?

02 Is the cyber security (risk) dimension another cause to be considered?

03 Do any additional hazards still map to the identified accident scenarios or have we identified additional accidents?

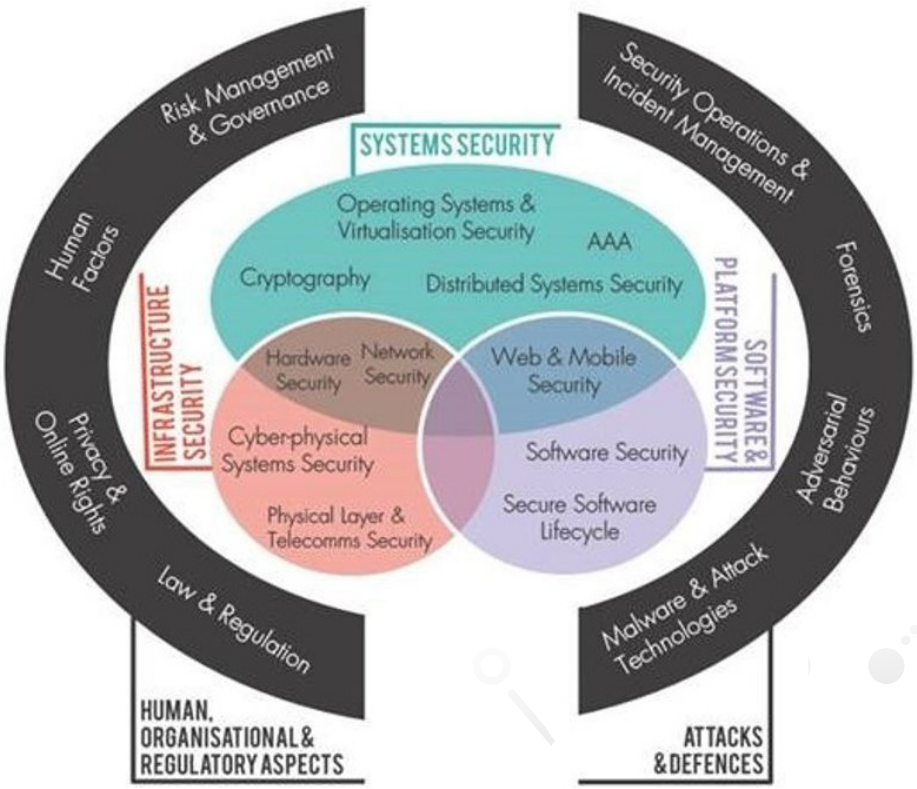
04 How does cyber security affect the current hazard log? Does it increase the probability or impact of the hazards?

03: INCORPORATING CYBER SECURITY

Fundamentally, there is an inherent lack of understanding of the characterisation of cyber security. There are many different definitions or explanations but, at CDS Defence & Security, we follow the structure of the National Cyber Security Centre (NCSC) and their 'Cyber Body of Knowledge' (right).

In very simple terms, it's about the compromise, either through external or internal threats, of information and information systems. The reason this is becoming so vital is the drive we now have for technology.

In today's fast pace defence development environment, you would be hard pressed to find a system, programme or piece of equipment in which technology is not used in some way, and where there is technology, there is a cyber security risk.



04: RISK MANAGEMENT

At its core, cyber security is all about risk management. Where cyber overlaps with safety, albeit using different terminology, is the consideration of 'safety to life' With safety, we're looking at causes and hazards which pose a risk to life, a very immediate causal chain which says if X happens, the risk to life will be Y.

However, risk impacts from a cyber security perspective centre on information and it's confidentiality, integrity and availability. Therefore, if a compromise does happen, the chain of events may not be as defined or immediate, but the risk is just as significant.

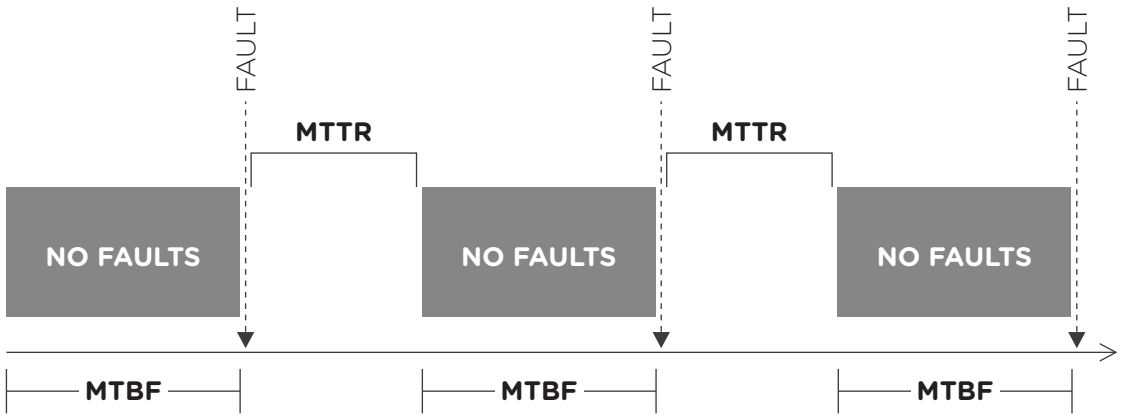
05: SAFETY TO LIFE

When considering and measuring the risk, we conduct threat assessments, we identify vulnerabilities and then we consider the various impacts - one of these being safety to life.

These assessments consider the inherent risk - that is the current risk with zero controls in place. We then look at the residual risk, for example, what could still happen despite those controls being implemented. It would then be the responsibility of the business as a whole to agree what their risk appetite and risk tolerance levels are.

The difference between the cyber risk assessment and the safety risk assessment is the lack of quantitive data. It's much easier to ascertain the probability of system failure due to the huge amounts of data created during exercises such as Mean Time Between Failure, calculating operating hours vs number of failures.

In cyber security, much of the risk is based on human behaviour and therefore it is much more difficult to predict when a breach might happen, meaning we can never accurately quantify the probability of risk.



SAFETY & SECURITY PROFESSIONALS WORKING TOGETHER

DEFINING SOCIAL ACCEPTABILITY OF RISK TO LIFE

AN INTERNATIONAL STANDARD COVERING SAFETY & SECURITY

UNDERSTAND AND SHARE APPROACHES USED BY BOTH

06: SO, WHAT NEEDS TO HAPPEN?

We've made our case. It's clear. Cyber security has a very real impact on the safety considerations of new defence equipment, but what needs to happen to ensure this is realised?

SAFETY & SECURITY PROFESSIONALS WORKING TOGETHER

By working together, safety and security professionals can give a holistic perspective of the challenges of developing new systems. Both disciplines focus on risk, and this common approach can create a synergy which saves both time and money later down the line, ensuring cyber security is not merely an expensive 'bolt on' when issues are discovered.

What is clear though, is that this is not a role or a joining of two disciplines which can be done by one person alone. Both are highly specialised, under resourced areas and so the most effective course of action at this point would be to use consultancy services from both sectors.

SOCIAL ACCEPTABILITY

In the safety world, 'broadly acceptable' is deemed to be an accident probability of one in a million deaths per year, making it socially acceptable to the wider public. If you can't achieve 'broadly acceptable' you have to show that you have done everything reasonable to reduce the risk to As Low As Reasonably Practicable (ALARP). And you cannot feasibly create an ALARP argument if cyber security is not factored into the equation.

CREATING A COMMON INTERNATIONAL STANDARD

Although there are currently a plethora of international standards across both safety and cyber, unless we create a unifying one which encompasses the two approaches, any action taken to mitigate risk will be open to individual interpretation.

cds
Defence
&Security

• The Bramery, 44 Alstone Lane, Cheltenham. GL518HE.
• 160 Rombourne, Aztec West, Bristol, BS32 4TU.

@CDS_Defence • enquiries@cdsds.uk • www.cdsds.uk