Your partner in progress

A BSI whitepaper

Technical Guide: Integrating Functional Safety and Cybersecurity

Assumptions and their Consequences

Contents

Introduction 3

Scope of this guide 3

Need for this guide 4

Benefit to the reader 4

Use of this guide 5

References 7

A Card Group - Properties 8

A.1 - System has no emergent properties 8

A.2 - Defending the network alone will naturally lead to resilience of the safety-critical functions. 9

A.3 - System is deterministic 10

A.4 - Focus on hardware 11

A.5 - Security must ensure functionality 12

A.6 - SIL 3 is better than SIL 2 in all circumstances 13

A.7 - All the identified risks are equal 14

A.8 - Safety sign-off of a system always implicitly includes a full and adequate security sign-off 15

A.9 - Failure is only due to malicious intent 16

B Card Group – Maintenance and Monitoring 17

B.1 - Expected measures for modifications 17

B.2 - Insiders aren't real 18

B.3 - All hazards and threats have been identified before starting 19

B.4 - It is obvious when I have been attacked 20

B.5 - Compliance makes me secure, and is possible in all circumstances 21

B.6 - Secure enough today and tomorrow 22

C Card Groups – Interfaces 23

C.1 - I can assume a perfect security boundary 23

C.2 - Perfect safety is assumed by security side and vice versa 24

C.3 - Environment is constant 25

C.4 - The automation architecture is completely documented 26

C.5 - Cybersecurity and functional safety measures do not interact 27

D Card Group – Supply Chain 28

D.1 - Product is delivered with integrity intact 28

E Card Group – Configuration 29

E.1 - Security integrity relies on secure components not configuration 29

E.2 - Multiple detection alarms will trigger corrective actions 30

E.3 - All functionality finds their source in a documented requirement 31

Authors 32

Introduction

Systems are becoming increasingly complex in terms of the operational technology and information technology used. These technologies are also becoming increasingly integrated into complex “systems of systems”.

With this increase in complexity, more robust measures are being developed in the functional safety and cybersecurity disciplines to counter the increasingly complex hazards and threats encountered. However, often these measures have historically been developed separately with little guidance or thought on the co-existence of the separate disciplines. This has led to largely incompatible assumptions and models in the fields of functional safety and cybersecurity, resulting from different simplifications of the world. The impact of this is that there is an increased possibility that hazards and threats are either overlooked or assumed to the domain of the other discipline. This could lead to a false sense of security and safety allowing incident to occur with increasing frequency.

Functional safety and cybersecurity experts globally are looking for additional interface mechanisms that allow for the consideration of each discipline without the need to alter existing working practices. Coupled with the commercial demands to improve productivity and shorten non-productive time, there is driving need for collaborative working.

This often proves to be as daunting as the problem itself, with complex guidance linked to extensive and intricate standards offering excellent yet difficult-to-understand information. Right now, there is still little practical guidance that can be used as a day-to-day guide to increase cooperation between functional safety and cybersecurity experts and how to avoid common mistakes and pitfalls.

Scope of this guide

This guide covers assumptions. These include pre-conceptions or assumptions which bias the process of achieving functional safety and cybersecurity. In this guide, common assumptions are highlighted, and a practical antithesis is offered to guide the reader to adopt good practice by challenging pre-conceptions in themselves and the wider team. This forms the foundation of good system development, operation and maintenance. The information is presented in a series of cards, and the tabular form offers an easy to use and check guide supporting planning of processes to ensure those processes are built with good practice and well-conceived initial principles.

Need for this guide

The principles of bringing together functional safety and cybersecurity in the operational technology domain have been successfully described by many previous standards and guidance documents. However, there is a need for a clear practical guide for practitioners and leaders on the integration of functional safety and cybersecurity resilience into existing processes.
This guide could require a change in user mindset and assumptions based on the lessons learned and the drivers for change experienced. This process should be structured, and guidance provided for all business stakeholders on how to integrate functional safety and cybersecurity.
Therefore, there is an additional need to challenge whether current practices are suited and how best to adapt and build the foundation from which the technical guidance can be implemented.

Benefit to the reader

This guide brings together the combined expertise of functional safety and cybersecurity experts from a wide range of public and private sector organizations and a wide range of technical and non-technical specialists to bring answers to the challenges posed by a combined functional safety and cybersecurity assessment.
This guide is suitable for all readers regardless of field and specialization, including engineers, systems, project management and operational management. Indeed, it is important for good system functional safety and cybersecurity that all work in a common manner.
This guide provides the basis for the common approach your business can take. The assumptions listed include indicator metrics which may be measured and tested as well as practical guidance and links to existing guides and standards to provide potential solutions or guidance on achieving good practice.

Use of this guide

This guide covers the assumptions made before and during a system's life cycle. This is useful at any point but specifically:

- **Conception**. At the very beginning of a project or organization where combined functional safety and cybersecurity measures are required, this guide will allow good practice to be implemented in business processes and systems.
- **Improvements, Upgrades or Maintenance.** When making changes to a system or organization this guide allows:
  - an assessment of the previous assurance case built;
  - building a better case moving forward and rectifying existing technical issues; and
  - simplifying the system without compromising the overall integrity.
- **Incident response**. This guide provides good starting assumptions when responding to an incident, whether it be functional safety or cybersecurity:
  - in the immediate response, how to effectively contain the issue without causing an additional weakness to become present; and
  - in the longer term, the improvements, upgrade or maintenance required by assessment of how the incident occurred, possible systematic and technical errors and how best to implement a long-term fix.

Each page is presented as a "card" to aid through decision-making processes. These cards can be used all together or individually. They are intended to provide key talking points for the following as examples:

- inter-department or business policy setting;
- technical review; and
- Key Performance Indicator (KPI) generation.

They are also intended to provide practical and understandable education and requirements for training.

To aid this, the cards are split into five groups. The properties group should be used at all stages of a system's life cycle, especially the conception phase as it allows for the implementation of a functional safety and cybersecurity by design. Other groups may be added to properties or used individually as required (e.g. system modification could be made by regrouping properties with maintenance and monitoring).

Group	Description	Card reference
A: Properties	General guidance on the expected characteristics and behaviours	A.1 A.2 A.3 A.4 A.5 A.6 A.7 A.8 A.9
B: Maintenance and monitoring	Ongoing activities to maintain functional safety and cybersecurity measures	B.1 B.2 B.3 B.4 B.5 B.6
C: Interfaces	The link between the safety, security and process systems	C.1 C.2 C.3 C.4 C.5
D: Supply chain	Considerations for procurement	D.1
E: Configuration	Control of configurations and version associated with safety and security measures	E.1 E.2 E.3

References

This guide complements existing information and best practices. In the preparation of this guide, the experts have considered a wide range of existing materials.

Below is the list of useful literature considered on this subject. These references are illustrative of the material available but should not be considered a complete list.

- **HSE OG-00086**, *Cybersecurity*
- 61508 Association — *Considerations for Cybersecurity during the Safety Lifecycle*
- NCSC/IET Code of Practice for Cybersecurity and Safety in Engineering
- **PD IEC TS 63074:2023**, *Safety of machinery — Security aspects related to functional safety of safety-related control systems*
- **PD IEC TR 63069:2019**, *Framework for functional safety and security*
- **ISA-TR84.00.09-2024**, *Cybersecurity Related to the Safety lifecycle*
- **PAS 7040:2019**, *Trustworthiness and precision of networked sensors — Guide*
- **NIST SP800-161**, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
- Professor Leveson's work on STPA and related work on how to incorporate security – aimed at the aerospace safety community but gets a lot of support among some in security. An intro to the work here: https://psas.scripts.mit.edu/home/wp-content/uploads/2016/01/Systems-Theoretic-Process-Analysis-STPA-John-Thomas.pdf
- US Department of Energy's Cyber Informed Engineering, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf
- https://www.oreilly.com/library/view/software-supply-chain/9781098133696/
- The NIST Cybersecurity Framework (CSF) 2.0, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- **EEMUA Publication 191**, *Alarm systems — a guide to design, management and procurement*
- **BS EN IEC 62682:2022**, *Management of alarm systems for the process industries*

A Assumption Cards - Properties

A.1 System has no emergent properties

The assumption

Designs often integrate “black boxes”, relying solely on supplier claims and on published interface specifications. Also, generally design and operate systems contain digital technology using simplified models while the true system complexity can give it hidden properties, outside the model. This arises because those systems are assembled from components using interface definitions that are incomplete. Interfaces can expose unused, undocumented and unexpected capabilities.

Why is this important?

The value of a system is that it can do things that its components cannot do in isolation; it is greater than the sum of its parts. These are its emergent properties. However, hidden component properties are inherited by the system and can generate further, unexpected emergent properties.

Functional safety analysis will therefore be incomplete; systems are so much more than the sum of their components. Security analysis will also be incomplete because adversaries could discover the hidden, undefended properties which might exploit them.

Indicators of the need to improve

A design mentality of integrating “black boxes”, relying blindly on supplier claims and on published interface specifications and a lack of “black box” integration analysis.

Functional safety and cybersecurity not engaging vigorously, together, with the design activity, as part of systems engineering at all levels.

How to proceed?

Duty holders should take responsibility for overall system operation and ongoing risk assessment. This involves informed dialogue down the supply chain. Manufacturers should be upfront about what they provide and the degree of novelty and complexity. Mechanisms to cope with emergent properties should be in place at all levels and these should be reviewed regularly.

References

NIST SP 800/160 Developing Cyber-Resilient Systems: *A Systems Security Engineering Approach.*

A.2 Defending the network alone will naturally lead to resilience of the safety-critical functions

The assumption

Defenders against attacks on digital technology can assume cyber-attacks are all network-based.

Why is this important?

Protecting an organization requires a multi-element defence-in-depth approach that provides resilience against all forms of malicious action, including blended attacks. Neglecting associated physical security, system hardening, endpoint security, user education and data encryption (just to list a few examples) exposes the organization to cyberattacks. Network security is just one element of defence.

Indicators of the need to improve

Conducting overly narrow risk assessments, being overly focussed on the assessment of network-based security controls, such as firewall audits.

Lack of comprehensive cybersecurity training programs for employees, e.g. on the breadth and range of cybersecurity controls. Poor communication and collaboration between IT security teams and other departments.

Lack of detailed policy or plan for expected system physical and software resilience for security and no visible validation of security measures (physical and software).

How to proceed?

Implementing a cybersecurity strategy to deliver resilience, including assessment of the performance of the broad range of security measures, such as set out in internationally recognized standards, across Protect-Detect-Respond. This can correct the pitfalls of relying solely on network security.

References

NIST Cybersecurity Framework 2.0

IEC 62443 (series), Security technologies for industrial automation and control systems.

A.3 System is deterministic

The assumption

Designers and operators generally assume that their systems behave deterministically, subject to individual component failures that can be modelled from the statistics of historical component failure data. This is not generally how digital technology fails, especially due to adversary action.

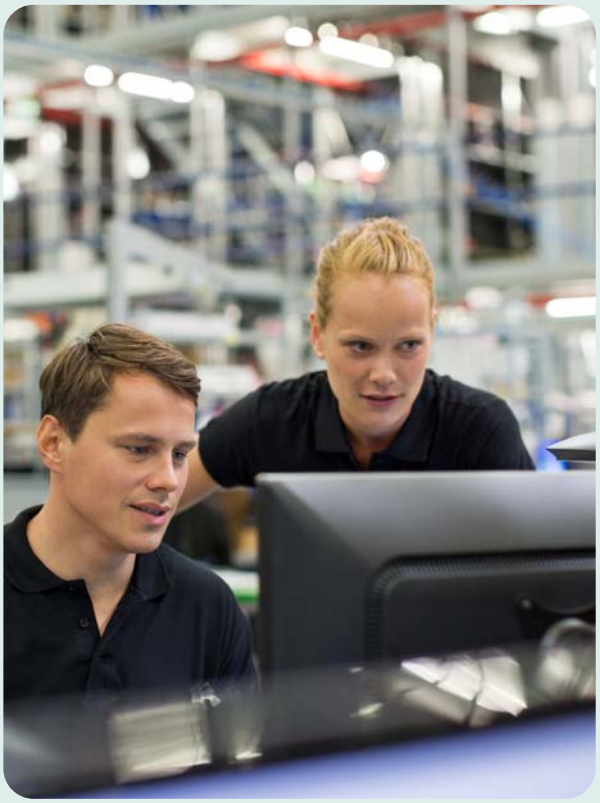
Why is this important?

Assuming that all failures and vulnerabilities may be determined could lead to the safety barriers and security controls being inadequate because the safety-related failure mechanisms are inadequately modelled. Given the degree to which it can be observed, a system can appear non-deterministic, especially at the edges of design conditions
or assumptions.

Indicators of the need to improve

Excessive reliance on generic tables of probabilities to predict failure rates for systems that contain complex digital technology. Assuming failure modes to be entirely predictable in all important respects using such models.

Overly focussed on failure rates and a lack of policy regarding the avoidance systematic failures and management of systematic risks. A more specific example could be conducting verification activities ad hoc, rather than in a planned manner.



How to proceed?

Ensure the system is designed and implemented to be as simple as possible, for the given functionality. Avoid excessive redundancy and system layers where possible. Where possible, make the system much more observable and design responses to foreseeable dangerous states. Be aware though that test points could introduce security vulnerabilities.

A.4 Focus on hardware

The assumption

It is common to be drawn to the tangible aspects of an activity because they are easier to analyse. This inevitably creates either an over-focus or an over-reliance on hardware aspects of systems.

Systems must be considered as an entity consisting of the tangible and intangible aspects, hardware, software, people, processes and the environment.

Why is this important?

An over-focus on hardware leads to the inadequate identification of safety barriers and security controls because the vulnerability and failure mechanisms are incompletely identified. Systematic and procedural failures must also be considered.

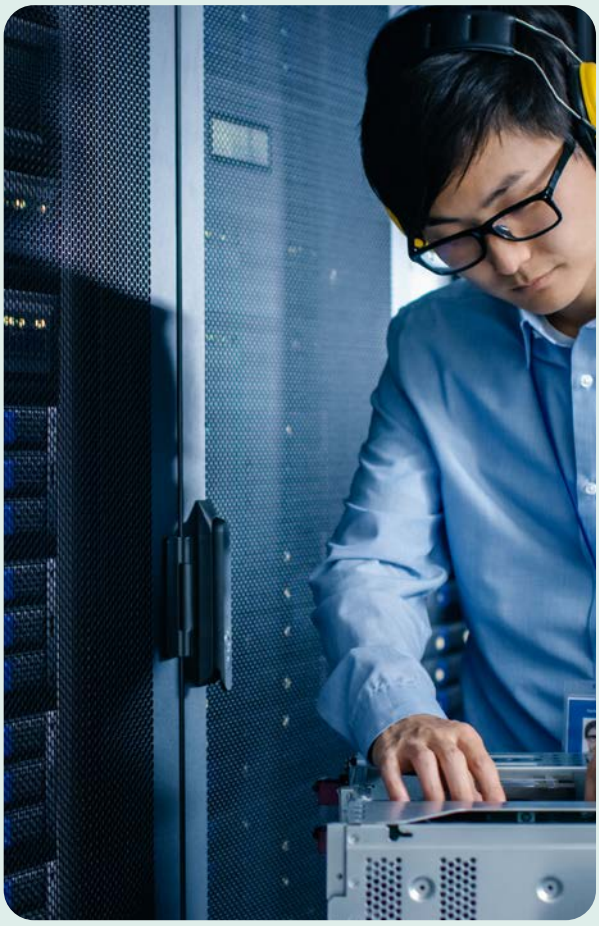
Indicators of the need to impr ove

The role of software and of people is under-represented in functional safety and cybersecurity analysis. The system is still suffering from compatibility issues and weak performance (low quality output, low availability). The functional safety and cybersecurity assessment appear to be entirely separate and utilize separate hardware to implement the measures.

Software, procedures and documentation within the systems is unchecked or only checked by one discipline. This is especially true where these services are brought in from external contractors. There is an over focus on hardware failure rates and not systematic failures. This can be seen through the use of tools such as FMEA to determine integrity based on generic or unverified vendor data without checking the quality of such data.

How to pr oceed?

Consider the human procedural and software measures as complementary to the hardware. Define the tasks and performance of the system. Utilize measures from security standards to identify how systematic failures caused by misuse and deliberate action might come about. Recognize that a random hardware failure cannot be foreseen. If the failure can be foreseen (e.g. software version loaded incompatible with hardware) this is likely to be systematic in nature. A site acceptance test or factory acceptance test needs to be performed in addition to the functional safety audits to verify the safety integrity and security level.



A.5 Security must ensur e functionality

The assumption

When considering functional safety and cybersecurity there is often too much focus on the “functional” part of functional safety and the “implementation” aspects of security. This leads to a split where the functional requirements purely address safety measures and the implementation requirements purely address security measures and there is no link.

Both functional safety and cybersecurity are whole life activities and require that functionality and implementation are correct to provide risk reduction.

Why is this important?

Failures are more often the result of honest mistakes or lack of knowledge, and effective security controls could deter or prevent that. Not every fault can lead to a system failure. Failures can happen due to one or more unaddressed faults. Security devices from different manufacturers might not be compatible with one another, leading to inability to deploy advanced security capabilities offered by those devices. Threats can occur due to hostile, inadvertent and well-intentioned reasons.

Indicators of the need to impr ove

A lack of visible or traceable assessment of risks or treats. An example is limited access controls or poor password management practices. A focus on deterrence over prevention. Frequent safety incidents or near misses. Resistance to security measures.

Formal reviews of the overall safety and security concept are not conducted. Frequent conceptual or specification changes, especially later in the design process, indicate a need to improve.

No policy on addressing functionality clashes prior to deployment. This often manifests as a continuous need for system modification, defects (“bugs”) not fix ed, lack of static and dynamic tools to capture non-compliant code to standards.

How to pr oceed?

Unify language for faults, failures, errors, hazards, attacks that are acceptable to functional safety and cybersecurity communities. Develop policies and procedures using a common and agreed dictionary of terms. This may be developed internally utilizing internationally recognized terminology.

Improve risk assessments to include consideration of failure modes due to minimal defences against inadvertent, careless or uninformed changes to safety and security configuration. Implement a diagnostic technique to detect hidden faults, proof testing to improve availability. Assess what system behaviours could induce ad hoc modifications.

A.6 SIL 3 is better than SIL 2 in all circumstances

The assumption

There is a common belief that a Safety Integrity Level (SIL) 3 capable component is always better than a SIL 2 rated component. Equivalent beliefs might hold for security targets (as defined in IEC 62443): bigger is better. However, each component must be suited to its intended application and over or under specification of a component could lead to unforeseen risks and consequences.

Why is this important?

Determining the proportionate degree of risk reduction is the critical criterion: too much and the reduction measures are likely to be onerous, constrain the operation of the component and parent system, or increase costs unnecessarily; too few and the system will not be sufficiently safe or secure.

Indicators of the need to improve

Specifying safety integrity levels and security levels without a sufficiently robust justification due to a lack of understanding of the link between risk reduction and design. No internal procedures for design based on risk assessments.

When there is difficulty in realizing functional safety and cybersecurity integrity requirements or excessive conflicts between domains this could be an indicator of over-specification of products without justification. Arguments for functional safety or cybersecurity that focus on SIL-capable components and Security Targets of components rather than on analysis of the resulting system are a likely cause.

How to proceed?

Robust risk management processes and understanding the underlying threats and risks are key. Understand the reasons for the risk reduction requirements and ensure the correct degree of rigor is applied. Target the lowest reduction required to satisfy tolerable risk criteria. Be clear on safety functions and zones. Understand functional safety and cybersecurity requirements for components and system.

A.7 All the identified risks ar e equal

The assumption

The identified risks will vary in their potential impact, likelihood of occurrence, and the ability to mitigate them. Those risks are also based on where the system is isolated or located in the network or at the core of a system architecture.

Why is this important?

Risks to safety and risks to security cannot be identified and treated in isolation. They both represent different types or views of risks to the same business functions.

Indicators of the need to impr ove

The identification of risks to information in isolation or the operation of systems in isolation, not calibrated against the impact to the business functions and outcomes of the organization.

Usually frequent and repeated security incidents, data breaches, regulatory non-compliance issues, plant shutdown, business disruption etc. indicates a need for improvement.

No evidence of a planned collaborative approach to implementation of the design.

How to pr oceed?

Corrective actions involve conducting thorough risk assessments, prioritizing risks based on their potential impact, and their likelihood, developing targeted mitigation strategies, and regularly monitoring and reassessing risks periodically.

A.8 Safety sign-off of a system always implicitly includes a full and adequate security sign-off

The assumption

Some people may assume that safety sign-off of a system always implicitly includes a full and adequate security sign-off. Such assumptions might not be true, as a safety sign-off of a system could be attempted solely by functional safety domain experts without involving specific security domain experts and therefore could lack appropriate consideration and validation when it comes to security.

Why is this important?

Risks to safety and risks to security cannot be identified and treated in isolation. They both represent different types or views of risk to the same business functions.

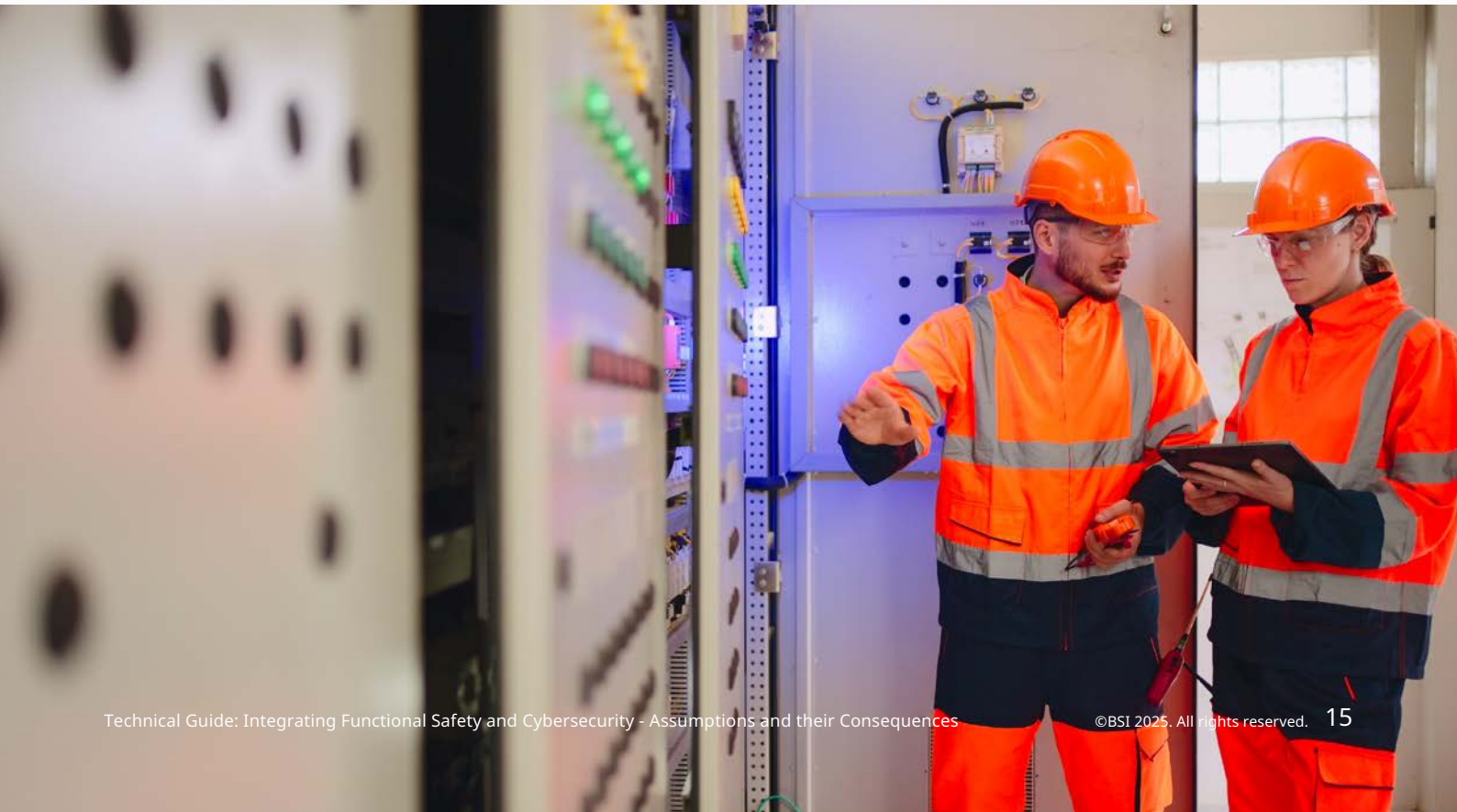
Indicators of the need to improve

Generally, a low degree of overlap in terms of assessment between functional safety and cybersecurity domain shows a need for improvement. Similarly, when the safety domain does not comply with recognized standards such as the IEC 61508 or IEC 61511 series, or assesses reliability rather than safety, this is another indicator for improvement. When security experts are brought in very late in the project compared to safety and general requirements derivation, this is a sign for a future failure. Finally, excessive conflicts between functional safety and cybersecurity domains should raise alert for a need for improvement.

No specific policy or plan or required competencies for the signing off of requirements for safety systems.

How to proceed?

Ensure functional safety and cybersecurity objectives are included and that appropriate domain expertise in both areas is involved in the project from definition to acceptance test.



A.9 Failure is only due to malicious intent

The assumption

Analysis of anomalous conditions can imply the cause is either a failure or malicious action and overlook mistakes by human operators.

Why is this important?

Functional safety and cybersecurity failures are often the result of honest mistakes or lack of knowledge. Effective verification process to the functional safety and cybersecurity control could provide evidence for proper implementation including scenarios containing foreseeable inadvertent human actions.

An example is the use of a USB Bluetooth or Wi-Fi dongle to temporarily enable OTA updates to a device. The dongle is forgotten and not removed, or the technician gets called away, leaving the dongle in place and an exposed threat vector.

Indicators of the need to improve

Poor verification practices, poor resilience against inadvertent introduction of threats (e.g. Human Factors).

Indicators include limited controls preventing unauthorized access, poor password management practises or a lack of training and awareness in the need to maintain cybersecurity measures in day-to-day operations. Other more physical indicators are unlocked panels or plant rooms, the sharing of login information and access cards to allow unauthorized users access for convenience.

How to proceed?

Ensure that within the organization there is a unified language on threats, faults and risk. Improve risk assessments to include consideration of failure modes due to minimal defences against inadvertent, careless or uninformed changes to configuration. Havea proper programme in place for procuring third party security devices. Assess what system behaviours could induce ad hoc modifications (e.g. spurious or excessivetripping or alarms).

B Assumption Cards - Maintenance and Monitoring

B.1 Expected measures for modifications

The assumption

When a system is in the design phase, there is a temptation to see the use case as immutable. This can lead to future modification requirements and procedures being overlooked and an installed system which is difficult to modify in a safe and secure manner or encourages bolt on modifications to overcome short term issues.

Why is this important?

It is possible to add vulnerabilities by the “back door” through undocumented component or system changes. Procedures to capture changes to the system must be robust to capture arising threats from apparently benign actions such as replacing devices or updating software online.

Indicators of the need to improve

The root cause analysis leading to the modification was not robust or conducted. A lack of Management of Change procedures for safety and security systems and regular audits to enhance procedures, or at the other end of the scale, a continuous demand for modification and changes.

Organizationally a lack of enthusiasm to introduce and manage improvements, or changes to existing processes even where there is evidence of deficiency.

How to proceed?

Review the specifications of the proposed changes, components, processes, etc. to ensure that vulnerabilities are not introduced. Check not just operating specifications, but the whole system specification and potential impact and degree of vulnerability.

Review of the modification process, change control, root cause analysis, affected phase, document, procedures, competency, role and responsibilities, and the existence procedures for better correction and prevention.

Review of incidents and changes made with a view to potential security impacts.

B.2 Insiders aren’t real

The assumption

All personnel with access to the digital technology are trustworthy. There is no need to account for “insiders” (those with authorized access and with malicious intent who have few if any barriers to breaching cybersecurity measures in place).

Why is this important?

Insider threats are a significant overall and cybersecurity risk with data showing an increasing prevalence of insider attacks. Attack planning scenarios should include details of common insider tactics.

Indicators of the need to impr ove

Absence of insiders from attack scenarios and an over focus on equipment failures. Organizationally dismissive attitudes, lack of or limited awareness of insider threat types, and weak password policies or practices. A lack of planning for incident response including the use of tools to limit data loss or monitor user activity.

Access controls and control procedures may be very poor. Indicators of this may include blank access cards, large groups of personnel having access to areas without necessity. Access to critical points without training and a culture of sharing access cards or codes informally.

How to pr oceed?

Increase awareness through training programs about different types of insider threats, their

motivations, and how to identify suspicious behaviour. Include real-world case studies of insider attacks to showcase the potential damage and the diverse profiles of attackers. Keep this up to date based on threat intelligence and the evolving tactics of attackers.

Strengthen security measures through application of the principle of least privilege, data loss prevention tools and user activity monitoring tools.

Maintain clear accountability for security and a clear policy on security measures and expectations.

B.3 All hazards and threats have been identified befor e starting

The assumption

Designers can assume that they are designing for a static operational environment, with all threats and hazards fully identified and resolved as part of the design. This is very unlikely to be true for security threats and might therefore be untrue for related safety hazards.

Why is this important?

Following a recognized hazard or threat assessment methodology does not guarantee all hazards and threats will be identified. Given that hazards, threats or both might be missed, or new ones later emerge during the operational lifetime, associated protection, mitigation or countermeasures will be missing. Due to the dynamic nature of vulnerabilities in digital technology and of security threats, the initial hazard or threat identification or assessment needs to be reviewed and revised. Those changes might have an impact on safety. Also, it is possible that the initial hazard analysis was incomplete.

Indicators of the need to impr ove

Absence of continuous reassessment of security risks and relevant policies and procedures. No evidence of detailed interaction between functional safety management and cybersecurity management systems.

Too little time, too few or inappropriate (i.e. lacking the required competencies) resources assigned to assessment of threats and hazards. Too little time between types or stages of analysis (e.g. HAZOP straight after HAZID). Limited detail in assessment and analysis reports resulting in loss of requirements. Too few initial functional safety and cybersecurity requirements.

How to proceed?

Ensure a strong functional safety management and cybersecurity management system interaction, reflected in management behaviour and organizational culture. Ensure the correct competencies are available at each stage of analysis/assessment. Provide guidance on threat assessment related to Security System/ Safety Instrumented System (SS/SIS) hazards.

Define response measures including escalation and de-escalation processes within the organization(s) involved. Identify threat-hazard characteristics and specific measures for potential unique cases.

B.4 It is obvious when I have been attacked

The assumption

A designer may assume that the operator will know promptly and unambiguously when the system has been attacked. There is ample evidence to show that this is rarely true.

Why is this important?

An attack can occur without detection until a negative impact is observed. Faults or failures and malicious attacks may present the same symptoms, which are difficult to diagnose in a timely manner. The response cannot wait until the initiating cause is clear.

Security breaches may remain undetected for some time (attackers may decide to stay stealthy, to pre-position, and launch an attack later for maximum damage).

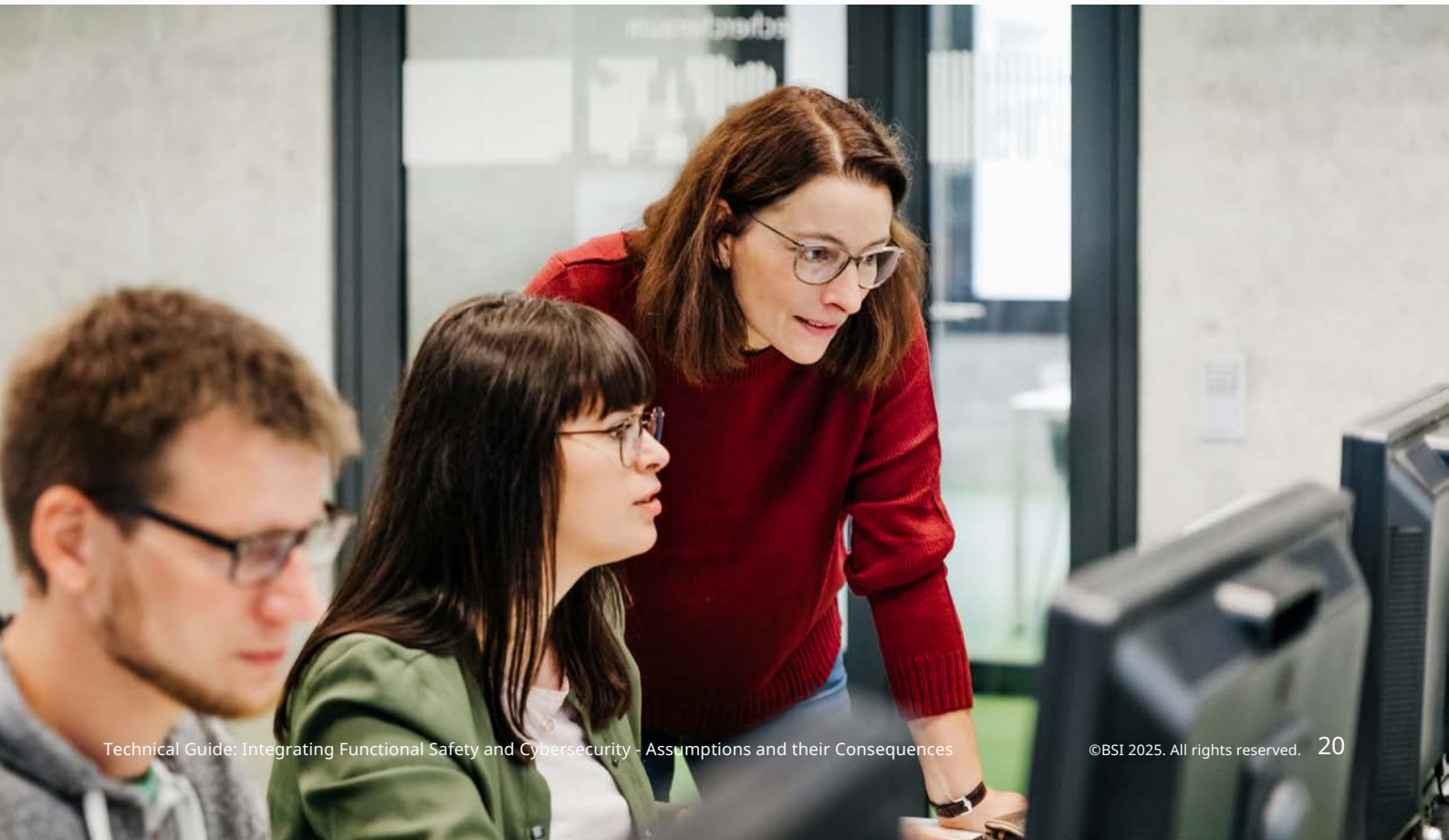
Indicators of the need to impr ove

Over-reliance reacting to events could lead to rushed or ineffective measures being retroactively applied. This is often coupled with a lack of defined security response procedures or procedures that start with the assumption that it is known how and when the system attack started. These measures might be of limited effect compared to a pro-active functional safety and cybersecurity approach.

How to pr oceed?

Keep an open mind. Combine security analysis with fault and failure trending and look for syndromes within the systems. Define response measures, plan for safety and security incidents including escalation and de-escalation measures. Test these plans in mock events if appropriate.

During a potential security incident, start with the possibility that the device could have been attacked rather than eliminating all other failure options and respond in a unified manner with parallel hypotheses of fault, failure or malicious action until resolved. Ensure there are robust failure and incident reporting mechanisms.



B.5 Compliance makes me secur e and is possible in all cir cumstances

The assumption

Some system owners assume that security standards contain all the necessary detailed descriptions of security controls to make that system secure, without interpretation. This is only true if the standard was tailored to the specific situation and the risks do not change.

Why is this important?

Absolute compliance with a detailed standard means the implementer is accepting the residual risk that was implicitly chosen by the standard writer. The writer assumes a set of assumptions about threat, consequences and system architecture. That could be the right approach where implementers can or must accept the rules defined by a competent authority who owns that residual risk. Nationally defined basic hygiene standards are a specific example of this. In circumstances where the system is unique, where system owners own the risks, blind compliance with a standard is unlikely to provide adequate protection.

Some might assume that compliance makes one secure or makes the system secure in all circumstances. This is not true as compliance means the system meets the quoted standard but standards can be out of date, inappropriate for the system and its (threat) environment, and/or applied or assessed inadequately.

Compliance to any standard helps reduce the number of potential issues, but it is not total assurance for a 100% issue-free system.

Compliance demonstration itself is subjective, and compliance does not guarantee cybersecurity or functional safety.

Indicators of the need to impr ove

Complex security standards cited by contracts with the demand that the vendor simply demonstrates compliance, without expecting assessment in the face of changing risks, and an explanation on why the result is proportionate.

When vendors and System Integrators deliver products or services to fixed standards that have no means for ongoing revision or updates. When duty holders or asset owners assume vendors and System Integrators have the risks covered.

Policies and processes for risk management activities with defined boundaries and potential interfaces (for example risk and competency management) are either not present or do not reflect the current activities and structures of the organizations involved.

How to pr oceed?

The risk owner for the system should expect to tailor controls to suit its circumstances and then maintain the means to continuously assess and manage risks with suppliers. This should cover vendors and System Integrators. Moreover, standards in use by stakeholders should be reviewed in accordance with the latest publication of those standards as new requirements might be added from time to time.

B.6 Secure enough today and tomorr ow

The assumption

Risk and threat reduction measures, once in place are sufficient only for a limited period of time and are not perpetually effective. The assurance of systems with a safety role is only valid as long as those systems remain static. However, software-intensive digital technology needs to evolve to maintain an acceptable level of security performance, as previously hidden vulnerabilities are identified and as new attack techniques are developed: what was sufficient yesterday is not sufficient today, no matter how much testing is done.

Why is this important?

The resolution to this apparent dilemma is to demand that systems with a safety role remain static while being protected by an adaptive security shield. As the emergent system properties and general continuing security requires restrictions on the design of functional safety systems, this is a model which cannot be effectively realized. This is a fundamental challenge to the assured, secure use of digital technology in systems important to functional safety.

Indicators of the need to impr ove

A clear definition and understanding of the system states and procedures to review, and if required alter, the system responses is not present. Measures which are present are not linked to current or emerging threat vectors.

Safety systems that do not change state when associated security responses move from PROTECT to DETECT and RESPOND.

How to pr oceed?

Build procedures and culture within the organization that promote a unified systems engineering approach which makes systems safe and secure throughout all their operational states. Consider the need to adapt both pro-actively and in response to events and how these actions might be triggered.

C Assumption Cards - Interfaces

C.1 I can assume a perfect security boundary

The assumption

Designers and operators claim a security boundary around a system for which everything it depends upon is within the boundary and all its adversaries are outside it.

Every system comprising software-based digital technology will always be developed from, normally continues to rely upon and often trusts other systems and functions that are outside designers' and operators' direct control. This means their system will have dependencies, trust relationships with entities outside their direct control.

Why is this important?

Risks to the performance of the system arise from dependences that cross the boundary from outside direct control. Specific strategies are required to identify and manage these dependencies, e.g. on the supply chain, on black boxes within the system.

Indicators of the need to impr ove

Interface assessments and change management assessment with clear assessment requirements are either not present or do not reflect the current state of the system.

Designers and operators devote most of their efforts to managing the risks that can be observed and controlled directly and neglect the higher uncertainty region (e.g. interfaces) which are beyond direct control

How to pr oceed?

Considering as part of the design how to manage risks arising from beyond the boundary of direct control including a plan for handling emergent risks and uncertainty. This could mean making the case to pay more initially to avoid later risk.

C.2 Perfect safety is assumed by security side and vice versa

The assumption

When designing a system, assumptions need to be made as a starting point. It is common to assume, when assessing risk in isolation or within a constrained scope, that risks outside one's scope are non-existent or adequately mitigated. This may be seen as a perfect measure scenario. However, rarely is this the case and the interaction between risk areas is critical to understand the overall risk profile for the system.

Why is this important?

Security experts might assume from the outset that the safety measures in their systems are ideal. This assumption could persist despite evidence to the contrary and security breaches will likely take place as a result.

Perfect functional safety and cybersecurity can never be assumed. It is a matter of when, not if, an incident takes place and the severity in terms of functional safety and cybersecurity.

Indicators of the need to improve

Teams working in isolation are unable to verify each other's assumptions and therefore tend to assume the best. Functional safety and cybersecurity teams collaborating is key to ensuring that assumptions made by one team are tested by the other.

Are functional safety and cybersecurity requirements derived from a holistic view of threats and risks, or drawn up separately based on previous experience?

How to proceed?

The functional safety and cybersecurity teams need to be able to collaborate, appreciate and test each other's assumptions. Leaders should consider location and timing of the activities and teams.

Where assumptions are made, these must be identified and recorded at all stages. Where possible avoid cut and paste requirements without first testing relevance.

C.3 Environment is constant

The assumption

During system development, especially software development, not fully understanding the environmental scope often leads to inadequate verification and assessment of the impact of the environment surrounding the system.

This leads to unexpected behaviours or failures during operation which could compromise measures taken to reduce risks and threats.

Why is this important?

Environmental (e.g. vibration, temperature) factors, or a lack of testing or lack of understanding of the application scope could result in a system that is not fit for the intended application. This renders the safety measures or security countermeasures ineffective in moderate to harsh environmental conditions.

Indicators of the need to impr ove

Inadequately defined requirements and requirements capture processes leading to the environmental condition not being considered or an assumed set of conditions used without supporting assessment or verification.

Poor availability typically due to continual failures or poor reliability. Requirements and specifications which do not capture all the environmental factors or are highly generic in requirements.

How to pr oceed?

Define the scope, range, obj ectives and intended end use of the system in detail sufficient to perform testing and verification utilizing known environmental assessment standards. Verify and validate functional safety and cybersecurity measures against the environmental specification and test as needed.

C.4 The automation architecture is completely documented

The assumption

It is tempting to assume that the automation architecture has been completely documented in a previous stage of the lifecycle. This is generally not true as in larger facilities (especially older ones) the automation equipment register might be incomplete and the interactions not properly documented.

Why is this important?

Analysis of risks is not representative to the real state of the system as it does not encompass the full architecture nor any updates or changes that might have been implemented over time.

Indicators of the need to improve

A lack of an asset register. A simple test of the existing asset register reveals errors and inconsistencies with the current state. Authoritative documentation is scattered among maintenance technicians or not even written and exists only in their heads.

Critical assets are not differentiated in the asset register or the definition of critical asset is not adequate or applied.

When asset owners or key personnel are changing roles or leaving the organization without a proper handover, this is a sign for an improvement. Similarly, when organizations are “discovering” systems or subsystems which are controlling key pieces of equipment, but nobody really knew they were present. This should raise an alert for a need for improvement.

How to proceed?

Set up critical asset management processes, namely asset register and management requirements. Define accountability for critical asset.

Audit the documentation and find out if there is a need for documentation update. Use a change management process that includes documentation updates and architecture review. Set up a handover process to avoid lack of knowledge and “discovery” scenarios.

C.5 Cybersecurity and functional safety measures do not interact

The assumption

Functional safety analysis will generally assume that the design and operation of security measures are benign to safety functions. The design and operation of security measures are assumed to have no impact on safety status.

Why is this important?

Cybersecurity and functional safety measures should reinforce one another by design and inform each other in operation. Security measures might detect anomalous behaviour in a control system that puts it outside its design conditions, or a poorly considered security response could actually cause this. Therefore, security designs could lead to safety failures when the cybersecurity and functional safety teams are not working together to achieve the common goals of resilience for the control system.

Indicators of the need to improve

Cybersecurity design and functional safety design are independent activities. Operational safety posture is generally not informed by changes to security posture, and vice versa, e.g. detecting anomalous behaviour to indicate that the system could be operating unsafely.

The discovery of organizational tensions and silos is key. These might manifest as a safety plan that does not mention security or vice versa, high levels of conflict resolution and arbitration. These often lead to functional safety and cybersecurity plans appearing very late in the process and in conflict with each other at the end

How to pr oceed?

Collaborative working is key. Ensure design requirements embody a system level approach that places equal and upfront emphasis on functional safety and cybersecurity. Allow the functional safety and cybersecurity experts to see and comment on each other’s work. Bring both into the project at the same (early) point.

D Assumption Cards - Supply Chain

D.1 Product is delivered with integrity intact

The assumption

Those who purchase products to integrate into their systems might assume that the product is delivered as intended by the vendor.

Why is this important?

Functional safety and cybersecurity domains are interdependent on one another. Assuming that a product fulfils both functional safety and cybersecurity requirement without thorough verification, can lead to the introduction of hazards or vulnerabilities. This assumption overlooks the potential for cybersecurity breaches to impact the safety of the product. Additionally, products could be delivered from a vendor via a complex supply chain and might have been compromised during that process.

Indicators of the need to improve

Vendors and their products are not subject to comprehensive security assessments or do not have robust functional safety or cybersecurity processes.

Risk analysis only considers more traditional safety failure modes and does not consider potential behaviour of products in the event of security compromise. Examples include mismeasuring or non-triggering.

The function or behaviour of a product might not be as the vendor intended at design. Additional or alternative capabilities of malintent could have been injected at some point during the supply chain, compromising system integrity and safety. Processes for verification of vendor products are insufficient or not in place.

How to proceed?

Conduct comprehensive assessments of supply chain security to gain confidence that vendors are applying good practices in their own design, development, sustaining, manufacturing, distribution and service processes. This will help to maintain the integrity of the product throughout its lifecycle and prevent any compromise during the supply chain process. Implement verification planning and execution for vendor products.

References

Crossley, C. (2024) *Software Supply Chain Security*, O'Reilly Media Inc. Available at https://www.oreilly.com/library/view/software-supply-chain/9781098133696/ (Accessed 16 September 2025).

National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf (Accessed 16 September 2025).

Institute of Engineering and Technology, *Code of Practice: Cybersecurity and Safety*. Available at https://electrical.theiet.org/guidance-and-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/ (Accessed 16 September 2025).

E Assumption Cards - Con guration

E.1 Security integrity r elies on secur e components not configur ation

The assumption

The addition of a security device, e.g. a r ewall, without conguring the de vice as well as the system it is protecting, can be assumed by some to provide the necessary security protection. This is rarely true.

Why is this important?

Security integrity relies not only on the presence of security devices or components but also correct congur ation of their features complemented by the congur ation of the control systems that are being protected. Incorrect congur ation of any could render security protection ineective.

Indicators of the need to impr ove

Supercial understanding of the performance of security devices. Absence of analysis of identity management, trust relationships and datao ws against current threats. Lack of verication and validation of security components after setup. Congur ation management is not in place or not applied consistently. Overall processes are not regularly audited, and updates are not actioned.

The use of insecure versions of protocols without explanation, e.g. HTTP instead of HTTPS (insecure and secure web protocols respectively).

How to pr oceed?

Proper validation and documentation of security congur ation during installation and commissioning. After each change is made, there is a means to assure that any congur ation changes are captured and procedures and documentation updated and the relevant stakeholders informed. Conduct routine auditing to conrm validity of measures.

E.2 Multiple detection alarms will trigger corr ective actions

The assumption

If a security device generates a notication, warning or alarm, policies and procedures assume there will be an operator with time and knowledge to assess it promptly and respond. This might not be true.

Why is this important?

In some sectors, the focus is very heavily on manual approaches and alarms to manage risk. In other sectors the approach is more automated but still relies on manual intervention. In the modern world, operators or crew do not usually have a lot of spare workload availability.

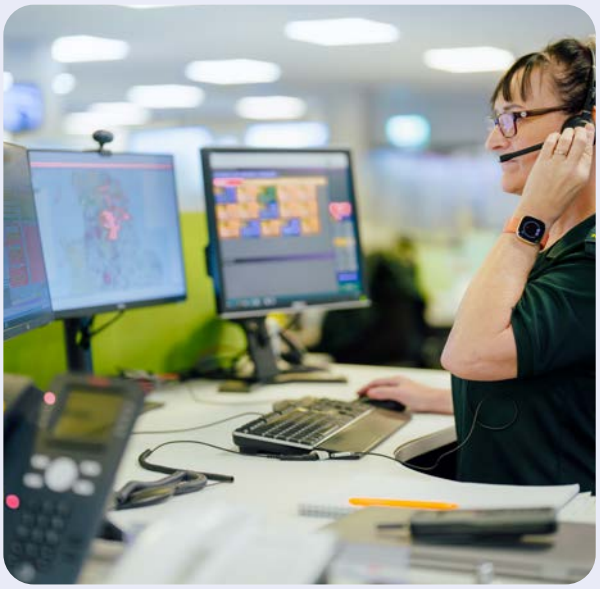
Alarms will be missed or ignored (basic human factors) at various times and situations. Alarm oods fr om unmanaged alarm approaches will hide important indicators of incidents. Attacks that trigger shutdowns or failures will produce many high priority alarms hiding security-focussed alarms. All alarms need careful alarm management (EEMUA 191, IEC 62282) and even then, only having an alarm might not be enough.

Indicators of the need to impr ove

Alarm oods ar e common, and operators or crew ignore alarms especially at times of stress or overload. Security incidents, both possible and real, are not noticed for signicant periods of time.

Alarm management is a low priority for the organization and no eective alarm management processes are in place, or these processes lack dened alarm r esponses.

No security consideration are made in the response to alarms.



How to pr oceed?

All alarms need careful alarm management and even then, only using alarms might not be enough to ensure a timely response to an incident. Separate out the safety-related and security-related alarms so that, where appropriate they have a higher priority than regular status alarms and procedurally, trigger higher levels of management.

Refer ences

EEMUA Publication 191 (2024), *Alarm systems: A Guide to design, management and procurement*. Available at https://www.eemua.org/products/publications/digital/eemua-publication-191 (Accessed 16 September 2025).

BS EN IEC 62682:2022, *Management of alarm systems for the process industries*

E.3 All functionality finds their sour ce in a documented r equirement

The assumption

An overfocus on the requirements generated for a system could lead to a blinkered approach which fails to take into account the changes made since the requirements were laid down as well as the human aspects of system development.

Not all functionality is ever captured; much is added ad-hoc or by user review and feedback. These, though often individually small, add up to signicant changes which whilst documented might not link to a documented requirement.

Why is this important?

Some might think that all functionality is related to the requirements. This might not be true, as requirements sets as originally derived are rarely complete. Moreover, during the system life cycle, requirements will need to be derived or changed.

Such static requirements might lead to vulnerabilities. For example, the requirement for a debug port available during production might be used as an attack vector during deployment if this requirement is not updated and removed.

Indicators of the need to impr ove

Usually, requirements analytics should indicate a level of change through the life cycle of a system. At the early stage, these will be very high and taper o thr ough realization or even be disabled through the deployment or production phase.

A lack of updates or processes to trigger reviews and updates will indicate that the requirements are not evolving.

Features not linked to requirements, especially where these are signicant featur e or functions, indicate a lack of formally documented functions.

How to pr oceed?

Derived functions and implementation features need to be retrospectively documented as derived requirements. Ensure requirements source is clearly dened and iterations recorded with justications including the need to change. Ensure eective change management is in place.

The Authors

This guide has been prepared by a drafting panel of the UK technical committee GEL/65 Measurement and Control and subcommittee GEL/65/1 System Aspects.

Jon Wiggins , Functional Safety and Cybersecurity Technical Manager, DEKRA (Chair)

Peter Br own , Functional Safety and Systems Engineer, Lloyd's Register

Tony Dodd , Software Development Manager and Product Architect, Servomex

Dr. Hassan El-Sayed , Business Development Manager, Functional Safety, UL International (UK) Ltd

Paulo Oliveir a, Director of Consulting, Process Safety, DEKRA

Mike StJohn-Gr een FIET , Independent Consultant

Dr. Karim T obich , Director, Cybersecurity & Technology Consultancy

Dr David W ard, Global Head of Functional Safety, HORIBA MIRA Limited

Dr Fan Y e, Technical Director- Functional Safety & OT Cybersecurity, WSP

Simon Lucchini , I&C SME, Cerilon Inc, (Member, ISA 5.1 Working Group)

Dur gesh Kalya , OT Security / Network Expert, Covestro LLC

Members of the BSI GEL/65 Functional Safety and Cybersecurity Drafting Panel

About BSI

BSI is appointed by the UK Government as the National Standards Body and represents UK interests at the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the European Standards Organizations (CEN, CENELEC and ETSI).

BSI traces its origins to 1901 and became the world's first National Standards Body. Its role is to help improve the quality, safety and integrity of products, services and systems by facilitating the creation and maintenance of consensus-based, market-led standards and encouraging their use.

BSI publishes over 2,700 standards annually and withdraws over 1,500 old or superseded standards using a collaborative approach, engaging with industry experts, government bodies, trade associations, businesses of all sizes and consumers to develop standards that reflect good practice.

To learn more about standards, please visit: www.bsigroup.com/standards and for the National Standards Body: www.bsigroup.com/nsb

Buy your functional safety and cybersecurity standards and a full range of other standards now at: knowledge.bsigroup.com

bsi Your partner in progress

Read more about standards at: knowledge.bsigroup.com