White paper: Cybersafety in the domain of voice communication systems

Ensuring safety and security go hand in hand in a highly connected world

As systems become more interconnected and the distinctions between internal and external processes continue to blur, organisations in safety-critical industries face a growing threat from IT vulnerabilities. These organisations wish to benefit from cost-effective, highly flexible open systems, but this openness potentially puts the reliability and availability of safety-critical voice communication at risk.

Based on real-world scenarios, this paper argues that it is vital to unite safety and security within an integrated architectural and organisational construct, and to address system security with system safety in a completely integrated fashion from the design phase onwards.

As the first step, to enable the smooth interoperation of different systems without exposing them to security issues, organisations should consider the division of their critical systems for information and communication into multiple distinct zones with tightly controlled perimeters. This will enable the appropriate balancing of safety and security requirements and their implementation across the specific assets and functions of the system. Beyond this, harmonising the management of safety and security will deliver ongoing benefits. Security in safety-critical industries cannot exist without a deep understanding and practice of safety within the DNA of the organisation.

Cross Industry

Opening systems to the world

Within safety-critical industries such as air traffic management, public emergency services, energy, and public transport, the availability and reliability of voice communication and control systems are crucial elements in assuring safety. In particular, mission-critical systems should not be overlooked. These tend to be found in military deployments and focus on the support of specific activities. Formerly, these systems were typically based on proprietary hardware and software running in complete isolation. Having effectively no connection to the outside world, such systems were less exposed to current IT security risks—and even where connections existed, the high degree of customisation gave external parties little or no chance of knowing about exploitable vulnerabilities.

As there was minimal potential for an IT security risk to have a tangible impact on safety, safety management was historically treated as a completely separate topic from IT security, and there was virtually no coordination at the architectural or organisational levels. Here, we define safety as the impact of a system on the environment, and security as the impact of the environment on a system.

Today, an increasing number of organisations in safety-critical industries are migrating communication systems to IP-based solutions running on commercial off-the-shelf (COTS) hardware, to take advantage of significantly lower costs for acquisition and operation. These open solutions also typically offer greater flexibility and usability, but not without some potential downsides. As systems become connected with other systems both internal and external, the potential attack surface and the number of exposed vulnerabilities are growing rapidly.

In the past, using proprietary hardware and software raised the bar for any potential exploits, for the simple reason that the technology was not widely accessible. By contrast, most solutions deployed today are based on technologies used by tens or hundreds of millions of users worldwide, making it easy for would-be attackers to gain the skills required to discover and exploit vulnerabilities. Like all other systems running on open platforms, voice communication systems face the threat of highly sophisticated malware, targeted attacks on common system vulnerabilities, and external events such as denial-of-service attacks—all of which may put safety at risk through their ability to disrupt voice communications.

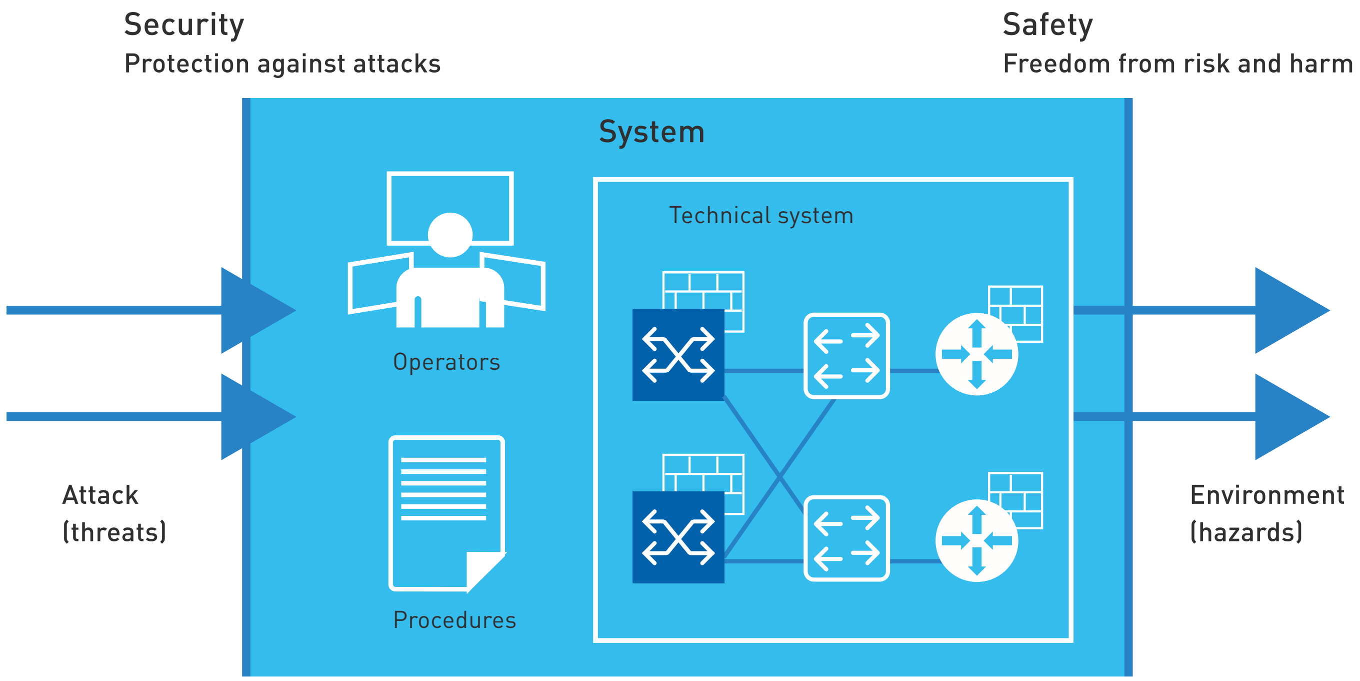
The link between security and safety

As a direct consequence of increased standardisation and connectivity, IT security threats have become a new root cause for safety hazards. Existing safety assurance procedures should therefore be considered incomplete if they do not call for appropriate measures to mitigate security risks.

Integrating IT security practices with safety assurance is not necessarily easy. For example, in certain scenarios, software-assurance regulations may conflict with security best practices around deploying critical system updates as soon as they are available. At times, organisations may feel that they are in a no-win scenario: should they disregard internal regulations by deploying non-certified software, or should they ignore critical security patches and run the risk of a serious incident?

Another issue is that the historical distinction between safety and security has driven an organisational wedge between the two areas. Many organisations therefore lack the structures and processes to work in a coherent way to ensure that IT security issues do not have a serious impact on safety.

Figure 1: Security and safety in the context of a system



Cybersafety – the harmonised approach

Based on long experience of deploying voice communication systems for organisations in safety-critical industries, Frequentis recommends the harmonisation of safety and security into a common and unified approach—termed 'cybersafety'—in order to reduce the risk of security events causing safety issues in the real world.

Safety assessments are an established feature within safety regulations. When applied to systems, they enable a proactive approach in considering and consequently minimising risk through hazard analysis, risk assessment techniques, and risk-mitigation methods such as the formalised failure mode and effects analysis (FMEA).

Security assessments provide mechanisms for controlling access to systems, with the goal of ensuring the confidentiality, integrity and authenticity of assets. By taking into account the potential safety impact of any breaches of confidentiality, integrity or authenticity for specific assets, organisations can create a formal link between the security assessment and the safety assessment.

By integrating the outcomes of safety assessments and security assessments into a holistic analysis of security threats and safety hazards, organisations can create an integrated system safety case. A safety case of this kind will present a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case, that a system is both safe and secure for safety-critical communications. Frequentis has seen promising results from taking this approach, backed by mutual understanding and closer cooperation between safety domain experts and security specialists.

IT security recommendations for safety-critical environments

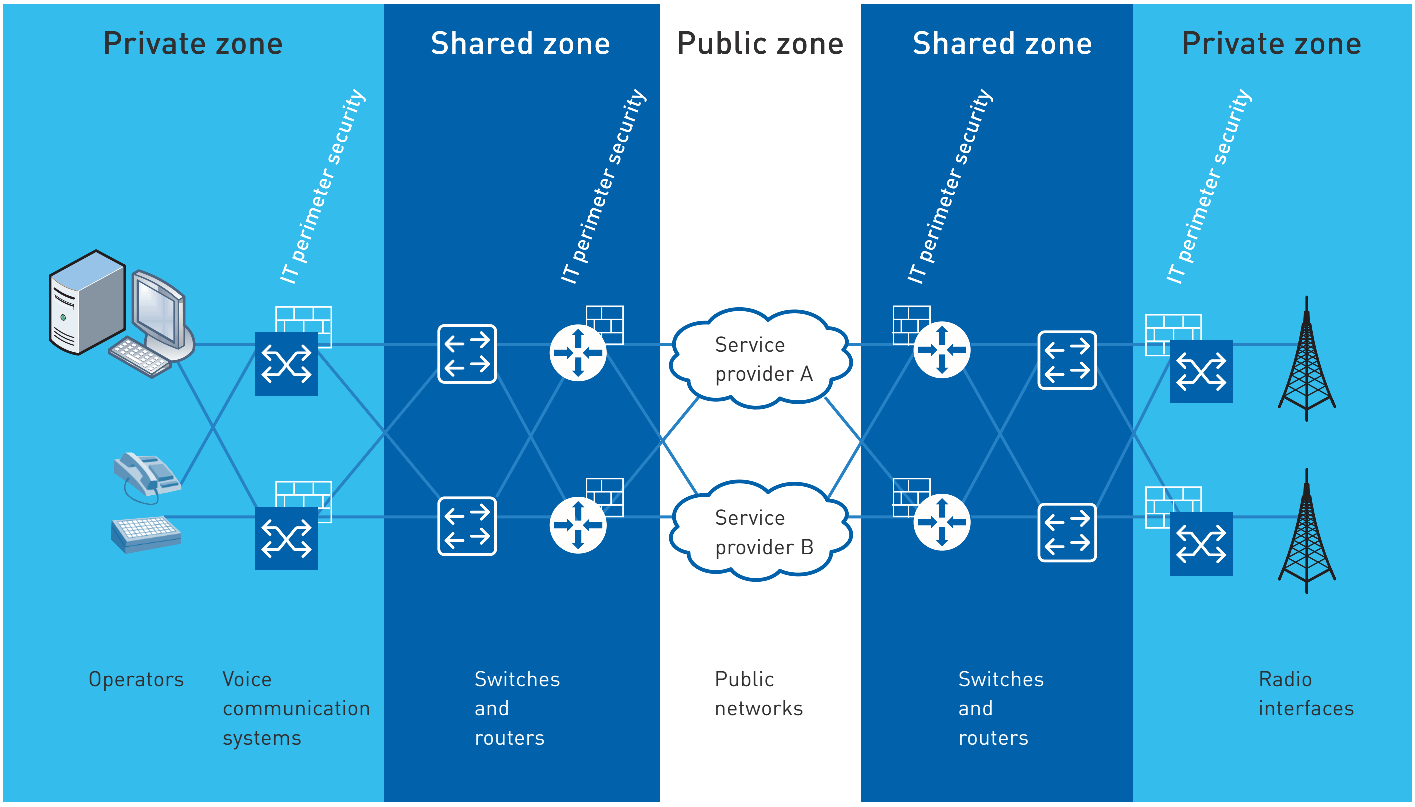
In practical terms, Frequentis recommends that the IT infrastructure be divided into at least three clearly defined security zones: public, shared and private (potentially with further subdivisions within each of these). Each zone groups together specific services that share a common level of trust and the hardware and software they are based upon. Analysing the assets and performing a combined assessment of the safety and security risks are shared responsibilities between the supplier of the safety-critical system and the organisation operating the system. Utilimately, it is the operating organisation's responsiblity to establish and monitor security within its own premises/data centre.

Determining the appropriate zones and their boundaries will require organisations to undertake a full analysis of all assets and the information flows they support.

Once established, the zones should be kept isolated using best-practice perimeter functions, including, for example, both physical and virtual firewalls.

Within the most private zones of the infrastructure, where systems are highly isolated from other zones, it will be possible to apply security updates less frequently. This can be done by ensuring that potential vulnerabilities are not accessible. If a vulnerability can't be accessed, it can't be exploited. This potentially eases the conflict between software-assurance requirements and security best practices—helping organisations to protect systems without needing to deploy updates before they are assured. Frequentis proposes that all safety-critical functionality should be located within private zones of this kind. Functionality that is deemed to be less safety-critical, and that requires a higher degree of connectivity and interaction with other internal and external systems, can be hosted within shared and public zones.

Figure 2: Security zoning for safety-related systems



Naturally, the appropriate allocation of functions and features to each respective security zone will require the integration of safety and security assessments into system design right from the outset. Organisations will need to undertake safety assessments, attack-surface evaluations, threat modelling and security-risk assessments during the design phase of any new system.

As would be the case for any mission-critical systems, organisations should put in place both physical protection for IT assets and system hardening for software and network resources. While the standard response to a network security problem might be to shut down the compromised area of the network, in this context it is vitally important to establish procedures that allow network security problems to be detected and analysed without blocking safety-critical communication functions. Incorporating considerations around IT security into safety assessments at the system-design phase will certainly start the organisation off on the right foot.

To achieve and maintain full harmonisation across safety and security, it will then be necessary to develop common processes and methodologies within an environment of cooperation and holistic management.

The benefits of a holistic approach

As IT security threats grow, organisations with safety-critical voice communication systems should unite their approaches to security and safety. By considering security and safety as interdependent rather than separate topics, organisations can better protect their systems against the safety implications of unplanned downtime.

Addressing security alongside safety during the system-design phase will improve confidence in systems. This is the basis for auditable evidence that the safety- and security assurance have been fully integrated from the outset. This design-led approach should be backed by efforts to create mutual understanding and close cooperation between experts in the safety and security domains. Finally, Frequentis recommends zoning the IT infrastructure to reduce the risk of a virtual security event having a negative impact on safety in the real world.

Organisations concerned about their existing approaches or about audit compliance can engage experts from Frequentis to conduct a comprehensive analysis of their infrastructure and provide practical recommendations for improvement. Safety is part of the Frequentis DNA and absolutely central to product development, deployment and ongoing customer support.

By taking a holistic approach to cybersafety for safety-critical voice communication systems, organisations can enjoy the lower costs, enhanced flexibility and easier connectivity of adopting open systems—without the potential downsides.

FREQUENTIS AG
Innovationsstraße 1
1100 Vienna, Austria
Tel: +43-1-811 50-0
www.frequentis.com

The information contained in this publication is for general information purposes only. The technical specifications and requirements are correct at the time of publication. Frequentis accepts no liability for any error or omission. Typing and printing errors reserved. The information in this publication may not be used without the express written permission of the copyright holder.