NO SAFETY WITHOUT SECURITY

Safety-critical infrastructures are attractive targets for cyber-terrorism. Frequentis' Christian Flachberger explains the need for effective cyber risk management and why preventative measures against future threats are being stepped up

The threat of terror in cyber space has developed at an alarming rate as terrorists continue to search for new vulnerabilities. Water, electricity, transport networks, emergency services and healthcare are all perfect targets for hackers wanting to cause chaos to critical national infrastructure. As these organisations have become smarter, more automated and interconnected, they have subsequently made themselves more susceptible to potential cyber threats through open and/or cloud-based solutions.

In response to an increase in targeted attacks, and persistent threats against critical infrastructures, governments worldwide have taken steps to increase security, setting new standards for security obligations. Critical infrastructure organisations must now provide demonstrable evidence for appropriate cyber risk management and regulators will have new powers to assess these industries, to ensure strategies to prevent successful attacks and plans for contingency are in place. They will also have the power to issue legally-binding orders to improve security, and, if necessary, enforce substantial fines. Consequently, the managers working in these areas need to ensure they are adequately protecting infrastructures or face being held accountable for security breaches.

Under the UK's Network and Information Systems (NIS) Directive fines could be as much as £17 million or four per cent of global turnover, with the penalties forming part of the governments five-year National Cyber Security Strategy (NCSS) to ensure the country's resilience.

CONFLICTING REQUIREMENTS

Applying cyber security practices from the business IT world for safety-critical missions is often in direct conflict with safety requirements, so many public safety end-users find themselves with somewhat conflicting safety and security requirements, yet, both must be implemented.

The problem of integrating safety and security requirements into one common solution is also a concern of industrial automation and control systems, widely used by critical infrastructures. Besides the well-known best practises of IT security, specific concepts for securing operational technology (OT) have evolved in this domain. IT security focuses on protecting data, while OT security is concerned with protecting operational processes.

In safety critical environments we suggest the introduction of protection zones within the technical system in order to apply the appropriate IT and OT security concepts to the right places.

Protection zones are defined as a collection of hardware, software and personnel with a common trust level. We suggest having at least three distinct protection zones with adequate isolation between them.

The internal zone is under full control of the organisation with dedicated resources (e.g. the network) and no direct connections to other systems. The shared zone functions with resources that are shared with another 'trusted' network. Connectivity is established to other, dedicated, operational systems. In this scenario there is linkage between two systems, but there is still no access to a public zone. A public zone is the part of a system with any connection to an untrusted environment, such as public network or third-party resources.

Different operational security practises can then be applied depending on the protection zone in order to focus on safety (internal zone) or on high connectivity (public zone). Examples are: frequent patching in the public zone, safety-assured software revisions in the internal zone; strict account lockout policy in the public zone (fail secure), monitoring without automatic lockout in the internal zone (fail safe).

STAYING SECURE

Keeping operational technical systems secure is a day-to-day management task requiring system operators and vendors to collaborate when completing activities such as cyber risk management, monitoring security warnings, applying patches, managing accounts, maintaining firewalls, monitoring the system to detect intrusions and so on. If the environment has changed and previous security assumptions have weakened it is essential to revaluate, perform a risk assessment of the changes and perhaps implement new measures to maintain the security of those systems.

The fact that many companies operate legacy systems which were designed and procured years ago means that although these systems may still provide up-to-date functionality and productivity, the landscape of cyber threats and the solutions for defending systems has changed. If the security of these systems has not been continuously updated it is advisable to carry out a security health check.

RECOGNISED RELIABILITY

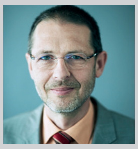
Frequentis has been providing highly reliable communication and information solutions in safety-critical applications for over 70 years. We regard security as essential for safety and began focusing on it a decade ago. We achieved the ISO 27001 certification for our integrated security management system in 2011.

We recommend a security health check and the selection of appropriate measures on a technical and administrative level through an understanding of safety and security as well as relevant IT and OT security standards. For us to provide secure systems we apply a secure development lifecycle, a security verification and a defined security handover.

The key to safeguarding day-to-day operations and keeping personal and operational data safe is an effective cyber threat protection strategy. There is no safety without security. ■

DR CHRISTIAN FLACHBERGER

Frequentis AG, Chief Information Security Officer/ Head of Global Information Security



Christian joined Frequentis in 1998, working in various roles from system engineer and technical project manager to security research team lead. He is now responsible for the group wide security strategy and its implementation across business areas and company locations. Additionally, Christian is a management consultant and security expert for the European Union.

FURTHER INFORMATION

www.frequentis.com