ACHIEVING RESILIENCE THROUGH THE

PRESERVATION OF FUNCTIONS

Safety and security working together

M. STJOHN-GREEN

Mike St.John-Green Consulting. Ltd

England, United Kingdom

Email: [mike@stjohn-green.co.uk](mailto:mike@stjohn-green.co.uk)

M. HEWES

International Atomic Energy Agency (IAEA)

Vienna, Austria

Email: [m.hewes@iaea.org](mailto:m.hewes@iaea.org)

**Abstract**

Advanced nuclear reactors, including Small Modular Reactors, promise enhanced safety and efficiency by harnessing complex digital technologies. However, these innovations also introduce risk management challenges regarding the computer security vulnerability of complex digital components to malicious action, faults and failures. Current nuclear industry approaches to safety and security operate with system-centric views, focusing on individual system robustness and redundancy. This approach does not explicitly address functional interdependencies, potentially causing gaps in understanding and addressing threats and vulnerabilities, resulting in a less efficient approach and less resilient result.

This position paper advocates a paradigm shift towards unified risk management whereby safety, security, and operational integrity are complementary aspects of achieving resilience through the preservation of functions. Although applying such a model poses analytical and complexity challenges, it provides a path towards more resilient nuclear infrastructure.

Recognising that safety and security fundamentally aim to uphold functional integrity facilitates collaboration between these domains. With the development of advanced nuclear reactors, the industry has a rare opportunity to develop new tools, techniques and working methods that foster cross-domain partnerships from the design phase onward. Ultimately, this integrated perspective on technological and organisational risk management will enable nuclear designers, regulators and operators to leverage the benefits of new and complex digital systems while ensuring robust safety and security.

## INTRODUCTION

This paper will use some examples of functions that are important to the nuclear security regime and consider how the design and construction of the digital technology to deliver those functions can be made resilient to malicious action, faults and failures by using a systems engineering approach. This approach produces systems that are secure by design, alongside being safe by design. This delivers a more effective and more efficient result than attempting to apply security in an additive manner to the digital assets, without adequate consideration of the functions they perform.

## What ARe we securing?

Conventional approaches to information security and computer security have often focused on, or have been interpreted as, securing individual systems, digital assets and the information they process through a set of discrete measures rather than defining and then meeting overarching security objectives to defend critical functions, such as reactor protection in a reactor [1]. This paper will illustrate how a system-centric view can lead to a fragmented and ineffective security posture, as it fails to consider the broader context in which these systems operate, the complex interdependencies between them, and the interweaving with other objectives such as nuclear safety. By prioritising the security of individual components through requiring compliance with a set of discrete measures without considering the larger picture, organisations may overlook critical vulnerabilities and fail to allocate resources effectively to mitigate the most significant risks.

In contrast, developing security objectives offers a robust framework for identifying and prioritising the preservation of critical functions. Safety and security objectives should be developed in tandem as the two are inherently linked - security must support safety and some safety objectives need reconciling with security objectives. For example, accident conditions could stem from violating a security objective, such as a malicious act against a system important to nuclear safety. The manner in which such a system is made both safe and secure may involve some systems engineering and architectural reconciliation to achieve both sets of objectives. Nuclear safety has a long-established culture of demonstrating adherence to a set of top-level objectives. Nuclear security should develop the equivalent approach.

Security objectives are materially different from the existing conventions established in safety, of protecting against faults, failures or accidents. Security needs to protect against intelligent acts delivered with malicious intent. Security is a continuously evolving struggle against knowledgeable adversaries who actively exploit vulnerabilities and launch targeted attacks to undermine critical functions, aiming to cause maximum disruption, at a time of the adversary’s choice. Many attacks will exploit weaknesses in the way assets and systems are assembled, compromising multiple layers of redundancy within a single attack, rather than in the individual assets alone. This requires that computer security is oriented to preserve the functions delivered by the combination, not just of the individual assets.

Organisations require continuous effort to maintain their security objectives and consequently security controls will not be static, in a manner that is similar to ongoing maintenance, required to protect against equipment failure. By framing security as a set of objectives, organisations can define the engineering activities necessary to achieve and sustain a desired level of trust in the reliability of their systems and functions they deliver against malicious acts. This focus on the design functions and on security objectives alongside safety objectives can also ensure designers consider initiating events that can fall between conventional security and safety analysis, such as errors by legitimate users that enable malicious action to undermine safety.

In the case of small modular reactors, many planned designs are expected to employ a much larger degree of digital technology than conventional reactors. The more widespread adoption of digital instrumentation, control systems, and human-system interfaces is expected to enable features like remote monitoring and maintenance, centralised control of multiple reactor modules, potentially remote operation, and even fully autonomous operation all requiring widespread integration of digital technology. For conventional reactors, most of the Instrumentation & Control (I&C) engineering has already occurred, and in many fundamental systems, structures, and components have been qualified and validated against safety objectives without consideration of supporting alignment with security objectives. However, due to a lesser prevalence and interconnection of digital technology, these systems can be demonstrated to be secured through only the sets of discrete security measures. For SMRs, this costly but fundamental engineering work is largely yet to be completed. Integrating security objectives from the outset, alongside safety objectives, will be essential to realising the benefits from the efficiencies offered by new digital I&C technology, while managing the risks arising from the increased prevalence and interconnectivity at an acceptable level and demonstrating regulatory compliance. This approach requires that security is viewed not as a post-design activity but as integral to the design and maintained throughout the lifecycle to ensure dependable, reliable, and trustworthy operations.

The following sections will review existing approaches to safety and security and advocate for a systems engineering approach to combine and resolve these two sets of objectives alongside the mainstream engineering objectives to enable designers, engineers, operators and regulators to see a unified approach to delivering efficient and effective safety and security in nuclear reactors.

## CURRENT APPROACHES TO SAFETY AND SECURITY IN ENGINEERING

This paper asserts that safety and security are often too disconnected in the engineering activities, specifically related to digital assets and that a paradigm shift is required towards unified risk management, within a systems engineering approach, where safety, security, and operational integrity are complementary aspects of achieving resilience through the preservation of functions. There is a wide range of ways this can happen, involving various disciplines that often work in isolation until (or after) final integration, leading to inevitable conflicts. This section describes some of the ways that this disconnect manifests itself. Consider the example of a digital instrumentation and control system that is designed to deliver against design function. Current approaches often use safety analysis to develop the design to the point that the safety case is acceptable. The analysis of failure paths, e.g. with a Bow Tie technique, identifies the need for barriers to maintain safety.

Where those barriers use digital technology, these digital assets become important to safety, attracting computer security requirements. The computer security team is then tasked to defend those assets against malicious action. The security measures are often assumed to be additive and applied around those digital assets without altering their safety critical functionality. With complex digital systems, this is at best inefficient and at worst impossible. Further, the adequacy of the security measures can too easily be judged against criteria associated with the correct operation of the digital technology rather than the correct performance of all the critical functions. The following simplified examples will illustrate some of the ways this can happen, and the suboptimal result for computer security and for safety.

### Example 1, Reactor Protection

Consider the Reactor Protection Function in a conventional Nuclear Power Plant (NPP), which intervenes to stop the reactor operating outside its design basis, to protect the reactor from damage. This may be implemented using a combination of mechanical and simple electrical systems. For the purposes of this paper, this function is delivered using digital technology, implemented in the form of two independent Reactor Protection Systems (RPS). There is a safety requirement that the RPS have a high degree of independent operation and will very likely demand separate digital hardware, separate power supplies, etc. Note that this NPP-related example is chosen because it should be widely understood, not because it is directly relevant to an SMR. The principles it illustrates are widely applicable, including to SMRs.

The security analysis will identify these two Reactor Protection Systems as being of the same criticality, because they perform the same function, and therefore they attract the same computer security requirements. Often, the computer security analysis will be focused on defending those digital assets against assumed scenarios of malicious action. Based solely on the need to defend the digital assets comprising the RPS, it would be logical to put the two RPS into the same network security zone, protected by common security devices. This simplistic approach to security would fail to defend the reactor protection function adequately because, if an adversary could compromise the common security device, the adversary would have access to both RPS. Example 1 illustrates how the computer security measures to defend the individual assets could be inadequate because they would create a single point of failure that fails to adequately support the safety requirements for the critical function.

### Example 2, Safety-critical cooling

Consider a safety-critical cooling function, such as to provide heating, ventilation and air-conditioning or to keep spent fuel rods cool. Let us imagine that the safety analysis determines the need for a separate layer of protection, independent from the process control. In this example, a designer proposes that the cooling function will be implemented using digital technology, with a SIL-rated Safety Instrumented System providing the required layer of protection independent of the Basic Process Control System (BPCS), in order to meet the required performance to meet the safety requirements for the cooling function. The designer implements this using a safety controller that is certified as capable of delivering to the necessary Safety Integrity Level (SIL). The safety controller sits in a card frame that provides it with power and communications. The BPCS is implemented in similar technology, in an identical card frame. The designer identifies options to save money, by having the SIS and BPCS share the same card frame and share some sensors, accepting the vendor’s assurances and proofs of independence to protect safety requirements, but without demanding corresponding assurances about the effects of adversarial action.

The safety analysis may consider this to be acceptable because the SIS card is built to be capable of operating to the necessary SIL level, irrespective of what else is in the card frame. However, this reasoning is flawed, as SIL-compliant devices do not automatically create a SIL-compliant system when wired together. Security analysis may simply demand that the combined card frame is protected to the higher security level, appropriate to protect the SIS. The vendor or designer may choose to demonstrate sufficient independence for safety, in light of reasonably assumed attack scenarios, but there is no guarantee this analysis will take place. The problem is only revealed if the security analysis (or systems engineers) go back to the original functional requirements and the assumptions made in the safety analysis, and check that there are adequate security measures to defend those assumptions of independence. If there is inadequate security analysis, the card frame may allow data-flows and trust relationships between the SIS and BPCS to be established by adversarial action. Example 2 illustrates how security measures could again fail to defend the assumed separation of digital technology, again violating the safety assumptions, because the security analysis was limited to the asset rather than the critical functions.

### Example 3, Safety Bow-Tie identifies the barriers for security to defend

Conventional safety analysis methods, such as fault trees or bow-tie techniques, have inherent limitations when applied to complex digital systems. Returning to the topic of Bow-Tie analysis, this is an example of what can go wrong with current safety and security approaches and illustrates the need to adopt a function-centric approach. Consider in this example the conventional safety analysis methods of failure analysis using fault trees or bow-tie methods. It is implicit in the way these methods are generally used that the paths are independent and can be analysed separately. Each barrier is assumed to be acting independently to stop failures causing a specific adverse outcome – the Top Event in bow-tie terminology. The barriers are not expected to be activated simultaneously.

In this example, the traditional security procedures call for security activity to be tasked to defend each barrier. However, a more comprehensive security analysis should consider an adversary that creates a coordinated attack that is designed to overcome multiple, parallel safety barriers in order to cause the failure of the function - the Top Event. Further, the security analysis should consider that the adversary can add functionality to the system, e.g. by covertly adding malicious code or hardware. This alters the system being defended and would warrant changes to the original bow-tie or fault tree analysis, if there were sufficient coordination between the security and safety teams. Therefore, more sophisticated security analysis may identify previously unidentified paths to cause the Top Event that should be fed back into the safety analysis. New adversary paths may also be created as a result of assembling the individual systems into systems-of-systems, which exhibit emergent properties. As digital control systems become more complex, there will be greater scope for emergent properties and consequently adversary paths that are created by combination of the systems.

## DEVELOPMENT OF A FUNCTION-CENTRIC APPROACH TO CSRM

An evolution enabling this systems engineering approach can be seen in the introduction of a function-centric approach to computer security risk management (CSRM) in the first revision of the IAEA's Nuclear Security Series publication, NSS 17-T Computer Security Techniques for Nuclear Facilities [2].

The original publication of NSS 17 focused on a system-centric approach to security, prioritising developing security requirements for individual digital assets without fully considering the larger picture, the interdependencies between systems and the properties that emerge from their combination. Implementations would see a standard set of computer security measures created at various levels of consequence within the facility. While the approach at the time was common practice within the nuclear industry, it led to an incomplete and inefficient delivery of security, with controls that were additive and targeted at protecting individual systems against compromise. The controls were not easily and demonstrably traceable to meeting security and safety objectives to protect critical functions.

The introduction of NSS 17-T Rev. 1 adopts a function-centric approach so that security measures defend the critical functions and, in this way, better support safety requirements. For example, the consideration of the critical function that a system contributes to would ensure that two systems on a common approach to defence in depth are separated into different computer security zones. This tailored defensive computer security architecture is designed to preserve existing approaches to safety defence in depth, providing a more effective and efficient security strategy.

The revised approach in NSS 17-T Rev. 1, while not describing the creation or interpretation of security objectives, provides a framework that recognises the interdependence between security and safety objectives, allowing the harmonisation of a computer security programme with the organisation's overarching mission and existing management frameworks. Doing so offers a more streamlined strategy for interpreting and implementing a mature and targeted approach to the security of functions compared to the original system-centric approach of NSS 17. Furthermore, it promotes a unified set of safety and security requirements, facilitating a consolidated requirements derivation process as part of an integrated approach to systems engineering.

There are others identifying the need to improve the manner in which security engages with the engineering process. For example, many organisations and States have Secure by Design initiatives, which call for security requirements to be considered as an integral part of the engineering lifecycle. The IAEA Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors (SMR/MRs) called for a One Team approach that would bring safety and security teams much closer in a systems engineering approach to resolve the issues described in the event [3]. Some such initiatives recognise the strong association with systems engineering and the need to consider functions, but, in comparison to the IAEA NSS, they retain a more system-centric approach, starting with the digital asset or system definition rather than having a strong function-centric starting point. [4] Some initiatives focus on the consequences of malicious action rather than on the critical design functions themselves. This is a subtle distinction, perhaps best considered security-centric rather than systems engineering-centric [5].

The central argument of this paper is consistent with the Secure by Design initiatives but goes further than many in calling for a function-centric approach. All these parallel initiatives can be seen as recognising aspects of the problem described in this paper and offering similar and often overlapping proposals to solve it. However, there is not yet an industry consensus on what this should look like. This paper argues that the true solution requires combining a function-centric analysis and harmonising security and safety objectives within a systems engineering processes from the outset.

## PRESERVING SECURITY IN THE ENGINEERING PROCESS

The paper will now return to the three examples and describe how a systems engineering based approach that defends the functions would have addressed the adverse results described earlier.

### Example 1, Reactor Protection

The requirements for independence of the two digital technology systems would be derived from the high-level requirements for the reliability and availability of the reactor protection function. These high-level requirements would flow to the security design team in parallel with the safety design team and the engineering design team. Those teams may not even be teams but a single, multi-disciplinary team. The architecture for the digital systems performing the reactor protection function would be tested against all the requirements, including those for integrity and availability of the function. The network architecture would be designed to maintain a high degree of separation between the two RPS and this would extend to using different maintenance laptops and other forms of diversity. This analysis would drive the security architecture.

### Example 2, safety-critical cooling:

This example also identifies the need for independence between the digital technology that is required to achieve a specified level of safety performance. A systems engineering approach would cause all the relevant requirements, including those for safety, to be correctly identified, to be flowed down from the designer and system integrator to the vendor. The vendor would have to demonstrate that the shared card frame offers sufficient separation between the SIS and the BCPS cards. This would overcome the problem whereby the vendor delivers a card frame, as an isolated system whose architecture meets a stated security level, without considering how to meet all the non-security requirements for resilience of the critical function that the system delivers.

### Example 3, Safety Bow-Tie identifies all the safety barriers

The challenge with this example is that the attack scenario assumes that the adversary changes the system, therefore any safety analysis must be reviewed in light of those assumed changes. This is unlikely to happen, given the current level of interaction between the safety and security processes. Moreover, there may be additional adversary paths made possible by the properties that emerge, such as by the additional functionality introduced by the adversary. A systems engineering approach, incorporating Secure-by-Design, will consider the effects of the assumed attack scenarios on the initial design of the digital system. Where those scenarios assume modifications to the system, such as by introducing malicious code or hardware, the final design should demonstrate how the security functionality will Protect-Detect-Respond quickly enough to maintain the Safety Case or alarm to inform the operator that the system has lost integrity due to a suspected cyber-attack. Note that this functionality includes not just preventative controls, under Protect, but the means to Detect and the full range of business processes to Respond, such as returning a digital asset to a ‘known good state’, following detection of malicious activity. These requirements may demand fundamental changes to the control system design.

## IMPLICATIONS FOR DESIGNERS, REGULATORS, AND OPERATORS OF SMRs

As digital technology becomes more complex, such as anticipated with SMRs, the historic approach of additive security becomes less and less efficient and effective. This is because computer security measures will increasingly demand changes to the digital architecture itself. To avoid this, safety and security requirements should feed into the systems engineering processes and those requirements be maintained throughout the system lifecycle.

These requirements should be traceable back to the functions that the system delivers, in order to assure that the function has sufficient resilience against all kinds of faults, failures and malicious action, throughout the system’s entire lifecycle. This requires a different mind-set, particularly for the security team, to work within a systems engineering regime, using a functional basis for managing requirements. It may also call for a different approach from the safety team, recognising that security cannot be additive, designed and applied as a layer around an existing design.

This means that the design teams for new nuclear plants, such as SMRs, must now include sufficient skills and knowledge to derive and maintain security requirements, alongside safety and engineering requirements. This may involve secondments of specialist computer security expertise into the design teams.

Maintaining the resilience of the functions during the operational phase, with engineering, safety and security working together, will prompt different relationships between the operational staff and incident response staff. Consider Example 1, Reactor Protection System for a nuclear power plant. It uses digital technology and at some point, the dual-redundant RPS then declares a fault because the two channels are in different states. This may be an operator error, an equipment fault condition or a malicious attack. Which team has the knowledge and skills to diagnose, manage and remediate this problem? Options include: the I&C maintenance team, the physical security central alarm station, the IT Security Operations Centre, somewhere else. The requirement for suitable alarms and alerts from the system should be designed in from the outset. There will be a requirement for suitably skilled teams to be created or adapted from today’s teams, organisational policies and procedures, authority hierarchies, and communications structures for incident responders.

Vendors will have their own part to play in this new approach. The developer of component digital assets and systems integrators who assemble assets into systems should become accustomed to seeing safety and security requirements in a more coherent and coordinated form, traceable back to requirements about the resilience of the function of that system or asset. The vendor is likely to have its own design team and the assets or systems will have their own lifecycles. Standards already exist for the certification of individual assets, e.g. within [6] and the other members of that family of standards.

The functions of those systems and assets should be assured in the face of faults, failures and malicious action by the system designers, system integrators and operators, as part of a system engineering approach. There are publications [4] and [5] that make relevant recommendations but there is as yet no consensus on the way to deliver the function-based approach called for in this paper.

Regulators frequently separate safety and security into different parts of their organisations, so there can be weak interaction between them, based on the premise that safety and security can be dealt with separately. Developing the coordination between the safety and security teams may be a challenge, but one that definitely needs to be overcome.

Those separations between the engineering, safety and security disciplines seen across industry can also be seen in the way IAEA guidance is developed.

## CONCLUSION

This position paper advocates a paradigm shift towards unified risk management, within a systems engineering approach, where safety, security, and operational integrity are complementary aspects of achieving resilience through the preservation of functions. Although applying such a model poses analytical and complexity challenges, it provides a path towards more resilient nuclear infrastructure. Recognising that safety and security fundamentally aim to uphold functional integrity facilitates collaboration between safety teams, security teams and engineering teams. If the arguments presented in this position paper are accepted, changes are likely to be needed to existing safety and security standards.

This approach has applicability to conventional NPPs but there is greater urgency to develop this thinking for SMRs, due to the likely reliance on new I&C technologies that have previously not been used in the nuclear sector. Others identify the need to improve the way security is achieved, with Secure by Design and other initiatives but there is not yet a consensus about what this looks like. With the development of advanced nuclear reactors, the industry has a rare opportunity to develop new tools, techniques and collaborative working methods. Once developed and established, this integrated approach will enable nuclear designers, regulators and operators to leverage the benefits of new and more complex digital technology while demonstrating traceable, robust safety and security.

References

1. INTERNATIONAL STANDARDS ORGANISATION, ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary, Edition 5, Geneva (2018)
2. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021)
3. INTERNATIONAL ATOMIC ENERGY AGENCY, Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors, <https://www.iaea.org/events/evt2100684>
4. Wright, V.L., Meng, J.P., Anderson, R.S., Gellner, J.R., Barnes, L.B., Chanoski, S.D., Edsall, R.M., Holtz, M.R., Jones, J.M., Le Blanc, K.L., Mahanes, J.C., McJunkin, T.R., Robinson, J., Rucinski, D.J., Shannon, G.E., Welch, J.J., Ayala, M., Atkins, V., Baker, K.A., Castillo, K., Cox, J., Gale, T., Graham, R., Groves, D., Johnson, S., Kishter, L., Macwan, R., Loo, S.M., McFly, S., Martin, M., Morris, M., Ohrt, A., Sachs, M., Venkataramanan, V., Waligoske, E., and Williams, G., “Cyber-informed engineering implementation guide”, 2023.
5. Freeman, S.G., St Michel, C., Smith, R., and Assante, M., “Consequence-driven cyber-informed engineering (CCE)”. United States: N. p., 2016. Web. doi:10.2172/1341416.
6. INTERNATIONAL ELECTROTECHNICAL COMMISSION, Security for Industrial Automation and Control Systems - Part 4-2: Technical Security Requirements for IACS Components, IEC 62443-4-2:2019, IEC, Geneva (2019)

ACKNOWLEDGEMENTS

The authors wish to thank Dr. Steve Essery (Method Cyber Security Ltd, UK), Mr. Jon Wiggins (1981 Consultants, UK), and Mr. Joe Mahanes (INL, USA) for their insightful feedback on the methodology, helpful challenges and suggestions. Any errors or omissions in the paper are solely the responsibility of the authors.