Security-Informed Safety "If it's not secure, it's not safe"

Robin Bloomfield, Robert Stroud

Security-Informed Safety

"If it's not secure, it's not safe"

Robin Bloomfield
Centre for Software Reliability
City University London
reb@csr.city.ac.uk

Robert Stroud
Adelard LLP
London, UK
rjs@adelard.com

***Abstract*— Traditionally, safety and security have been treated as separate disciplines, but this position is increasingly becoming untenable and stakeholders are beginning to argue that if it's not secure, it's not safe. The idea of combining safety and security is not new but neither is it straightforward. To illustrate the complexities of the problem, we explore some of the challenges that need to be overcome in order to develop a principled approach to "security-informed safety".**

Keywords—security-informed safety; assurance cases.

I. INTRODUCTION

For a system to be safe, it also has to be secure. Otherwise, a safety critical system – one that can harm or injure people – could provide attackers with a potential mechanism for causing widespread damage or panic, and it is credible that such systems could become the target of malicious actions.

In principle, achieving interworking between safety and security should be straightforward. Both are sophisticated engineering cultures that emphasise the need for good process, the importance of risk analysis and the need for assurance and justification. However, these similarities are superficial and in practice there are significant challenges, as experience with large-scale systems has shown.

To illustrate the complexities of the problem and in order to stimulate debate, we explore some of the technical issues involved in combining safety and security assurance in a principled way. Our work is informed by an investigation of these issues in the context of the railway industry [1], but is more widely applicable to safety engineering in general.

II. CONCEPTS

The commonalities between safety and security are frequently obscured by the use of different concepts and terminologies. Indeed, there is considerable variation in terminology both within and between the safety and security communities. Thus, to achieve a shared understanding of the key concepts within each domain, there is a need to establish a lingua franca or even a common ontology.

The IFIP WG 10.4 dependability taxonomy [2] offers some hope for defining a consistent set of terms. In particular, it makes a clear distinction between cause and effect and highlights the need to be clear about system boundaries.

Broadly speaking, safety is concerned with protecting the environment from the system whereas security is concerned with protecting the system from the environment. Security and safety can both be viewed as kinds of dependability and use similar techniques to identify potential failure modes and assess their impact on the overall system. Thus, there is considerable overlap between safety and security methods, although the focus is different and in some cases safety and security requirements can be in conflict.

In particular, one of the major differences between safety and security is that a secure system needs to cope with evolving threats and changes to the environment through design and architectural measures as well as operational ones. It is important for the system to remain safe and secure despite such changes, in other words, to be resilient to change.

III. PRINCIPLES

There are many overlaps between safety and security principles, but there are also some significant differences in emphasis and some potential conflicts. For example, defence in depth is an important architectural principle for both safety and security that depends on the use of multiple, and as far as possible independent, barriers. However, security considerations are likely to challenge the effectiveness and independence of safety barriers.

From a safety system perspective, security principles [3] such as economy of mechanism, least privilege, and psychological acceptability are probably all readily acceptable. Other principles, such as complete mediation and end-to-end arguments, could have a significant impact on the architecture and performance of systems. But perhaps the most radical security principles from a safety perspective are those based on Kerchoffs' principle [4], namely ease of recovery and open design.

In particular, although safety systems are already designed to support operational changes for calibration and maintenance, the ease of recovery principle, which states that the security of the system should not depend on anything that cannot be easily changed, could have far reaching impact on the architecture of safety systems.

Moreover, changes to threats over the lifetime of the system will probably mean that controls that were adequate initially will need to be reconsidered. This has implications for

This research was commissioned on behalf of UK government and the UK rail industry.

the architecture and lifecycle of embedded safety systems where design life may be 20-40 years.

Given the uncertainties around future threats, systems should be designed to be adapted and replaced perhaps sooner then would be necessary from just a safety perspective. This could have significant architectural and cost implications for large infrastructure projects, particularly those that are already in progress

IV. METHODOLOGY

Risk assessment is a fundamental step in safety and security analysis, but the underlying threat model is different. There is a need for a unified methodology for assessing the threats to the safety and security of a system.

Security considerations can have a significant impact on a safety case. For example, there needs to be an impact analysis of the response to security threats and discovery of new vulnerabilities and reduction in the strength of protection mechanism. This suggests a greater emphasis on resilience of the design.

It is also necessary to consider the potential for attack during a safety incident and the opportunity this might provide for malicious activity. A fail-safe state may not be as safe as previously thought if the system is under attack and the assumption that any security attack on a control system could only, at worst, cause a fail-safe state to be reached is in general not true. Moreover, assumptions about the capabilities and state of society may change; for example, consider managing a safety incident during a major security incident.

Given the importance in security of open scrutiny of design and implementation (e.g. of crypto), it is an appropriate question whether security-informed safety cases in entirety or part should be disclosed. Within the safety community, the principle of independent assessment is well established, but the design details within a safety case are usually considered to be confidential and are not made public in their entirety.

The key question is whether publishing the detailed design and safety analysis for a system would make the system less or more safe and secure, or more precisely which aspects would it be beneficial to expose and which not.

V. STANDARDS

Safety standards already require *"malevolent and unauthorized actions to be considered during hazard and risk analysis"* [5], and there have been a number of domain-specific attempts to define a unified approach to safety and security assurance [6][7]. However, the standards framework for dealing with security-informed safety needs to be more explicitly designed than is currently the case. In particular, the relationship between generic and domain-specific safety and security standards needs to be clarified, and terminological and conceptual differences need to be resolved.

The standards framework should be based on explicit principles and use a consistent terminology. The standards groups should ensure they have available a suitable mix of both security and safety expertise.

Standards often use "levels" as a way of classifying systems, risks and controls. However, it is important to understand the assumptions that underpin these classification schemes and not to confuse different kinds of classification. In particular, risk levels, requirement levels, and assurance levels need to be carefully distinguished.

A particular concern is the problem of justifying requirements that specify the use of particular methods and tools to achieve a specific level. In order to support interworking between safety and security standards, we need to develop a better understanding of the rationale for such recommendations and the evidence base that supports them.

Security standards are often based on security controls, a concept that embraces a wide range of different interventions covering process, product and organisation. In contrast, safety standards are typically based on an engineering life cycle model. In principle it should be possible to relate safety mitigations to security controls, but in order to perform such an analysis, it will be necessary to define a common way of classifying controls and mitigations.

VI. NEXT STEPS

We believe that some or all of the following next steps would be helpful in establishing a more principled approach to "security-informed safety".

- Develop guidance on concepts and terminology to support dialogue between the safety and security communities.
- Research the applicability of security principles to safety and the associated trade-offs and conflicts.
- Consider how to make credible arguments that safety and security risks have been reduced to as low as reasonably practicable.
- Investigate how a Claims-Arguments-Evidence based methodology could be used to support the development of a security-safety protection profile.
- Intercept and support the standards process in order to clarify the relationship between safety and security and resolve some of the terminological and conceptual issues.

REFERENCES

[1] R. E. Bloomfield and R. J. Stroud, "Safety and Security: Concepts, Standards and Assurance", Adelard reference D/719/138002/2, v2.0, March 2013.

[2] A. Aviziensis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing", IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, January-March 2004.

[3] J. H. Saltzer, M. D. Schroeder, "The Protection of Information in Computer Systems" CACM Vol. 17(7), July 1974.

[4] A. Kerckhoffs, 'La cryptographie militaire', *Journal des sciences militaires*, vol. IX, pp. 5–38, Jan. 1883, pp. 161–191, Feb. 1883.

[5] EN 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General Requirements.

[6] Praxis High Integrity Systems, SafSec: Integration of Safety & Security Certification, November 2006.

[7] ED-202, Airworthiness Security Process Specification, EuroCAE, December 2010.