Addressing security in safety projects – experiences from the industry

Bjørn Axel Gran, Anne Egeli, Alexander Bjerke

Addressing security in safety projects – experiences from the industry

Bjørn Axel Gran
Department of Production and Quality Engineering
NTNU
Trondheim, Norway
bjorn.a.gran@ntnu.no

Anne Egeli, Alexander Bjerke
Safetec, an ABS Group Company
Oslo, Norway
{anne.egeli, alexander.bjerke}@safetec.no

***Abstract*—Security and cybersecurity has become familiar to everyone. Nevertheless, security is still some-thing that often denoted as not applicable when companies are developing or operating programmable electronic safety systems. In this fast abstract we try to point of some of the reasons to why it is like that, and discuss the problems by both believing there are no reasonable foreseeable security threats, and by believing that every thinkable attack can hit you. We also describe how we as consultancy try to address security in safety projects, and how guidance address the challenge. Finally, we point to the role of system owners that manage to set up clear expectations to include and integrate both safety and security**

Keywords—safety, security, industry

I. INTRODUCTION

Over the two last decades, security has become a phrase common for everyone work-ing with programmable electronic critical systems. Going back to year 2000, the EU-funded CORAS project "A Platform for Risk Analysis of Security Critical system" [1] was one of the first large projects addressing security in critical applications, driven by seven field trials within telemedicine and e-commerce [2]. Today, the number of security related projects are large. There is also a so wide range of relevant standards so that it becomes wrong to mention one and leaving others out. Although security has become familiar to everyone, security is still something that often is denoted as "NA" (not applicable) when companies are developing or operating programmable electronic safety systems. One aim of our research is to point of some of the reasons to why it is like that. The other aim is to propose some ways to address security in safety projects in an appropriate way based upon experiences from consultancy work in different Norwegian industries.

II. BACKGROUND

Protection from terrorism or other intentional crimes is denoted as security, while safety implies protection from unintentional acts. The difference lies in whether the incident is inflicted intentionally or not; safety risk is characterized by being accidental and security is characterized by being intentional or deliberate. This implies that, in the case of security, an aggressor is present who is influenced by the physical environment and by personal factors [3]. At the same time that security has become familiar, there have in the academia been a discussion if it is meaningful to distinguish between security and safety as to separate fields of handling risks and crisis [3, 4, 5].

III. 3 WHY IS THEN SO HARD TO INCLUDE SECURITY IN SAFETY PROJECTS?

There is a number of good hints and advices on the need of including security also in safety projects provided in a number of international generic and branch specific standards. On the other hand, the experience from working in different client projects within the process industry and transport over the last years tells that it is not that easy. Often security aspects are not addressed at all, or they are addressed rather late in the design and development process. An important question is then why it is so hard to include security in safety projects.

A. Specialists in the security field believe that safety and security are two different phenomenon

Jore and Egeli demonstrated some answers to this question in a study [5]. During the spring 2014 they interviewed 15 informants representing 10 different institutions within the oil and gas sector. Five informants worked exclusively with security, while the rest worked with both areas of safety and security. The aim of the study was to generate new in-depth knowledge on the topic of security risk management that can contribute to the development of better security risk analysis methodology. Two findings from the study were:

- 9 out of 15 informants are in favor of specific risk management methodology for the area of security. All informants working exclusively with security supported this argument.
- 8 out of 15 informants claim that probabilities cannot be used in security risk analysis. All informants working exclusively with security supported this argument.

One observation from their study was that specialists in the security field believe that safety and security are two different phenomenon, and they should be approached in different ways. This statement is supported by the lack of historical data for security risks and in particular for security risks such as terrorism. For other security risks, this is not the case. A security crime that most petroleum companies and other businesses presently have to be prepared for is cybercrime. For

this type of threat, an enormous number of attacks occur every single day, so there are numerous data available for risk analysts. This would also be the case for other types of security risks, such as burglaries or other types of more "ordinary" crimes. For those security risks where a large dataset exists, these should be included in the risk analysis, although it would be necessary to consider the relevance of these data.

In practical risk management, a company has to address both the area of safety and the area of security. Petersen [6] studied the role of security professionals in cooperate businesses and concluded that security professionals in an organization often are not fully incorporated into the main tasks of the organization. This can have as consequence that they also use risk management methodologies that are not consistent with the rest of the organization. Research has also shown that companies' anti-terrorism policies are often not based on a normative treatment of risk that incorporates likelihoods of attacks. Policy makers' anti-terror decisions may be influenced by the blame they expect from failing to prevent attacks [7].

B. *Specialists in the safety field believe that there are no security threats*

Requirement 7.4.2.3 in IEC 61508 [8] says: "If the hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out". There is however a problem. The ones that are responsible for the functional safety management are the specialists in the safety field. Firstly, they lack historical data for security risks and in particular for security risks such as terrorism. Thereby they conclude that it is not reasonably foreseeable. Secondly, they may lack the needed guidance, as security is not the main topic of the safety standards, and the number of applicable security standards are large. Finally, they may lack the knowledge about the threats. Actors conducting illegal operation in cyberspace vary from government intelligence and security services, traditional military adversaries, global commercial companies, terrorist- and extremist groups, to organized hacker groups. Motives can include idealism, criminal activity, terrorism, economical gains or geopolitical considerations. To understand how and why an actor can be a security threat, it requires the safety specialist to have insight in the motivation, the mission, the mindset and the methods of the attacker. Hommedal states that every security professional should have a strong understanding of these four M's [9]. However, to be applied in the safety projects, this understanding is also needed within the safety professionals.

C. *Some Common Mistake Specialists in the safety field believe that it is just a question about the vulnerabilities*

The requirement 7.4.2.3 can also be answered with that everything is reasonably foreseeable. In that case, the next step is to undertake a vulnerability analysis. In many projects, this means to address a set of security standards. This is observed done in two ways: (i) use the requirements in the standards as guidance, or (ii) use the requirements as compliance requirements.

The first strategy works fine since it may imply to first address the threats, then establish some reasonable scenarios and finally ask what kind of means and barriers that should be included. The problems comes when the requirements in the security standards are included as list of requirements that should be complied to. Firstly, this may lead to having security requirements that are in conflict with the safety requirements. This means that this assessment should have taken place early in the project in order to solve the conflict. Addressing it later may mean that it is impossible, or to costly, with the results that the security requirement is dropped. Secondly, this strategy do not address the threats. This means that there may be a larger number of security requirements and barriers that are included, while other security needs are overseen.

IV. CONCLUSION AND FURTHER WORK

Security and cybersecurity has become familiar to everyone, but security is still something that often is denoted as "NA" (not applicable) when companies are developing or operating programmable electronic safety systems. In our research, we try to point of some of the reasons to why it is like that. We discuss both the problems by believing there are no reasonable foreseeable security threats, and by believing that every thinkable attack can hit you. We believe that one of the main challenges for the industry is to balance safety and security risk management, and find ways to integrate security risk in the overall risk management.

REFERENCES

[1] CORAS. A platform for risk analysis of security critical systems, IST-2000-25032, 2000 http://coras.sourceforge.net

[2] Fredriksen R., Gran, B. A., Stølen, K., Djordjevic, I.: Experiences from application of mod-el-based risk assessment. Proceedings of the European conference on safety and reliability (ESREL'2003) vol. 1, Swets & Zeitlinger, 643-48 (2003)

[3] Reniers, G. L., Cremer, K., Buytaert, J.: Continuously and simultaneously optimizing an or-ganization's safety and security culture and climate: the Improvement Diamond for Excel-lence Achievement and Leadership in Safety & Security (IDEAL S&S) model. Journal of Cleaner Production, vol. 19, no. 11, 1239–1249 (2011)

[4] Pièrre-Cambacédès, L., Chaudet, C.: The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety". International Journal of Critical Infrastructure Protection, vol. 3, no. 2, 55–66 (2010)

[5] Jore, S. H., Egeli, A.: Risk management methodology for protecting against malicious acts – are probabilities adequate means for describing terrorism and other security risks? Safety and Reliability of Complex Engineering Systems, Podofillini et. al (Ed), Taylor & Francis Group, London, 807-814 (2015)

[6] Petersen, K. L: The corporate security professional: A hybrid agent between corporate and national security. Security journal, vol. 26, no. 3, 222–235 (2013)

[7] McGraw, A. P., Todorov, A., Kunreuther, H.: A policy maker's dilemma: Preventing terrorism or preventing blame. Organizational Behavior and Human Decision Processes, vol. 115, no. 1, 25–34 (2011)

[8] International Electrotechnical Commission (IEC): IEC-61508. Functional safety of electri-cal/electronic/programmable electronic safety-related systems (2010)

[9] Hommedal, F. See it coming: The Four M's of Digital Espionage. Published at LinkedIn 21.september 2014, (2014)