REVISITING THE RELATIONSHIP BETWEEN SAFETY AND SECURITY

NEKTARIOS KARANIKAS
Aviation Academy, Faculty of Technology, Amsterdam University of Applied Sciences, Netherlands.

ABSTRACT
Safety and Security (S&S) have the same goal, that is to maintain the integrity of human, infrastructure, hardware, software, capital and intangible assets of a system. However, literature and practice indicate that the relationship between S&S has not yet been clearly defined and their boundaries remain blurry. The current paper presents a short review of academic and professional literature about the relationship between S&S. This relationship is examined by looking at the S&S dependencies, their similarities and differences, and the role of the human element in achieving and maintaining the desired S&S levels. The review of literature showed that (1) there is a tendency to emphasize on the effects of security on safety and underestimate the opposite, (2) human factors are not part of security training to the extent are addressed in safety training, (3) security and safety problems can be the result of both internal and external disturbances and agents, (4) the intentionality or not of outcomes, and not of the action, can stand as a valid criterion to classify an event as a security or a safety one correspondingly, (5) S&S issues can result in negative implications internally and externally to the system, and (6) the synergy between S&S is of paramount importance for achieving the optimum levels of system protection. The positions of this paper might comprise a basis for enriching educational programmes around S&S and igniting relevant research.
Keywords: safety, security

1 INTRODUCTION

Safety and Security (S&S) have the same goal, that is to protect a system and maintain the integrity of human, infrastructure, hardware, software, capital and intangible assets. Burns *et al*. [1], Cusimano and Byers [2] and Blanquart *et al*. [3] explained that S&S are mutually dependable because a safety problem might cause a security issue and vice versa. Fletcher [4] viewed S&S as emergent properties of modern complex systems and argued that since the 9/11 event S&S have become even closer to each other due to their association with system design and operation. The proposition of Fletcher [4] was the establishment of a fully integrated global security and safety management system, a concept Stoneburner [5] had highlighted as a means to overcome the security-safety dichotomy.

Blanquart *et al*. [3], under the reality of limited resources, suggested to prioritise higher the security controls needed for risks that might lead to severe safety implications, a practice called "security for safety" and aligned with the perspective of ABB [6]. In the same line of thinking, Hahn *et al*. [7], referring to the chemical process domain, stated that both physical security and cybersecurity guard system safety. If cybersecurity fails to prevent data corruption, computer viruses and other infectious attacks that can be spread through networks, then control systems will be affected, and the safety of workers, the public and the environment will be jeopardised along with system efficiency.

2 SIMILARITIES AND DIFFERENCES

Burns *et al*. [1] focused on the intentionality or not of adverse consequences to classify an event as security-related or safety-related correspondingly. Dahlstrom and Dekker [8] noted that S&S have different focus areas since security refers to intentional acts and safety to

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://www.witpress.com/journals
DOI: 10.2495/SAFE-V8-N4-547-551

unintended consequences, and can even conflict such as in the case of the locked cockpit door. In their work, Piètre-Cambacédès and Chaudet [9–10] introduced the System-Environment-Malicious-Accident (SEMA) framework to address the ambiguities regarding the S&S notions. The SEMA framework is based on two distinctions: System vs Environment and Malicious vs Accidental. Security risks are malicious, originate from the environment and might impact the system, whereas safety risks are accidental, arise from the system and might impact the environment. Aligned with Piètre-Cambacédès and Chaudet [9–10], Baird [11] added the argument that, in safety risk management, a product that is easy to use is often safer to use, whereas, in security risk management, a product that is easy to use is usually exploitable.

Firesmith [12], amongst others, developed a model for safety and one for security and demonstrated that the specific domains deal with different cases, but their concepts are closely related. Particularly, Firesmith [12] concluded that safety is about preventing events caused by hazards (e.g., carelessness, hardware failures and natural phenomena), whereas security is about repelling threats and attacks. On the side of similarities, S&S strategies are grounded in the fundamental risk management cycle that considers the assessment of risk levels based on probability and severity estimations, generates requirements to prevent or reduce the effects of hazards/threats, and introduces responses to bring the system back to its normal state after a risk event [12].

ABB [6] saw safety problems as results of unacceptable risks of damage to people, property or the environment, and security problems referring to illegal or unwanted penetration, interference with proper operation or inappropriate access to confidential information regardless of motivation (intentional or unintentional) or consequence (result). According to Dahlstrom and Dekker [8] and Hancock and Hart [13], on the one hand, both S&S focus on managing risks, involve trade-offs to achieve a balance between protection and production goals, and they bring value to business and customers not immediately visible. The latter occurs because the number of adverse events prevented is unknown and people cannot easily perceive the notion of "non-events". Fuller [14] suggested that, in the supply chain domain, an effective transportation risk management shall balance S&S with operational efficiency and ensure that operational staff understand, accept and adjust when S&S causes inconveniences. An integrated approach to S&S would be feasible through a combined S&S risk assessment as suggested by Cusimano and Byers [2].

Young and Leveson [15] stated that in current practice S&S are recognised as different system properties, and each of them is addressed through its vocabulary and models. The same authors articulated that safety experts concentrate on the prevention of unintentional actions by benevolent actors whereas security experts manage risks related to intentional acts by malevolent actors. Young and Leveson [15] suggested that security analysis must move from the mere consideration of behaviours of individual system components to a more systematic top-down approach, namely STPA-Sec, that allows a systems view and an examination of system controls and dependencies. The specific approach sources from the System Theoretic Process Analysis (STPA) technique which was first introduced for safety analyses of complex socio-technical systems [16].

3 THE HUMAN ELEMENT

Despite the fast and continuous developments in technology, the human element remains a critical part of our systems and inevitably plays a decisive role in maintaining and improving S&S. It seems that this has been recognised in the security domain since decades, as, for

example, indicated by the study of Neiderman and Fobes [17] who presented a cognitive model of the perceptual and cognitive processes involved in X-ray screening. Based on the specific model, Neiderman and Fobes [17] suggested a set of 51 psychometric tests for the proper selection of X-ray screeners.

Hancock and Hart [13] proposed the consistent application of human factors and ergonomics principles and solutions to the design, manufacturing, and operation of technical security systems as well as all homeland security areas. Such principles include staff performance assessment, signal detection, vigilance, monitoring, alertness and perception of operators, team performance, selection and training, and emergency response. The authors mentioned above viewed such an approach as promising in improving passenger and luggage screening effectiveness in aviation and resolving conflicts generated due to the demands of airlines for faster and less costly security checks.

In 2002, the International Civil Aviation Organization published the document titled "Human Factors in Civil Aviation Security" [18] where the crucial role of human factors in security was recognised. The areas addressed by the specific document are selection, training, assessment and retention of personnel, use of technology in security operations, consideration of the operational environment and organisational culture, and certification. Nevertheless, Dahlstrom and Dekker [8] claimed that, apart from technical and operational aspects, the security domain can further benefit from the experience gained from human factors as a means to render security safer for staff (i.e. persons who implement security measures) and customers (i.e. persons who are subject to security measures) as well as more effective. In addition to enhanced safety and effectiveness, knowledge and recurrent training in human factors topics such as individual, team and system limitations and effects of automation on human performance, may support the maintenance of skill, awareness and readiness levels necessary to deal with security events.

4 REMARKS AND CONCLUSIONS

The literature reviewed denotes an agreement about the mutual dependency between S&S. However, it also indicates a tendency to focus more on the effects of security events on safety. The latter perspective seems to neglect that a safety issue might generate system holes which can be exploited for security breaches. For example, the failure of a system component used in normal operations can cause a fire, which is classified as a safety event but it can also damage security controls (e.g., surveillance cameras).

Importantly, the effects of the various human factors, which have been for long part of academic and professional safety education and training, especially regarding high-reliability and safety-critical industry sectors, have been recently considered by the security domain. It seems though that the security field has not yet emphasised on themes such as individual and team performance, coordination, over-automation effects etc. that comprise areas of continuous safety research and education.

The viewpoints about the similarities and differences between S&S are quite diverse and somewhat confusing and partially contradictory. The various opinions mentioned in literature seem to address three areas of differences: the aim of the S&S activities, the origin of the agent to be prevented, intentions of the particular agent, and impacted areas. When attempting to reconcile the positions of the authors cited in this paper, it can be concluded that:

- The scope for both S&S is the protection of the integrity of a system so it can sustain operations and produce services and/or products within defined standards.

- Regardless of the labels given to agents, such as hazards or threats, those can be external or internal. Safety problems can occur due to inappropriate or inadequate system behaviour and control, but also because of excessive disturbances from the external environment. Security issues usually arise when external agents attack a system, but an attack can even be executed from within a system (e.g., the assassination of Indira Gandhi by two of her bodyguards in 1984).
- When referring to the intentions of the agents, typically humans, the emphasis on actions does not seem standing as a valid criterion. Many safety events have occurred because the end-user(s) intentionally performed actions, which in hindsight proved to be wrong. However, it can be claimed that intentionality can comprise a classification criterion when it refers to the outcomes. Strangely though, the crash of the Germanwings flight 9525, which was deliberately caused by the co-pilot, was investigated as a safety event.
- Although the precise definition of the system under consideration is of vital importance for defining what constitutes external environment, the System-Environment distinction suggested by the SEMA framework to categorise an event as security-related or safety-related neglects that (1) there might be malicious agents within a system as discussed above and (2) there is a potential of a safety event to vastly and negatively affect the environment or being initiated by it (e.g., the Fukushima Daiichi nuclear disaster in 2011).

In addition to the remarks stated above, the necessity for a standard S&S risk management framework and model has been pointed out and supported by recent developments such as the STPA-Sec technique which is an adaptation of the STPA technique used for safety analyses. What is highly important though is the synergy between the S&S domains as a means to effectively use the resources devoted for system protection, highlight to management the inevitable S&S compromises when production targets prevail under given capacity levels, and resolve possible conflicts when developing and implementing S&S controls. When a system's integrity is lowered due to any reason, the overall risk escalates, and all system properties might be affected.

REFERENCES

[1] Burns, A., McDermid, J. & Dobson, J., On the meaning of safety and security. *The Computer Journal*, **35**(1), pp. 3–15, 1992. https://doi.org/10.1093/comjnl/35.1.3

[2] Cusimano, J. & Byers, E., Safety and Security: Two Sides of the Same Coin, available at www.controlglobal.com (accessed 3 November 2017).

[3] Blanquart, J.P., Bieber, P., Descargues, G., Hazane, E., Julien, M. & Léonardon, M., Similarities and dissimilarities between safety levels and security levels. *Proceedings of the 6th European Congress in Embedded Real Time Software and Systems*, ERTSC, Toulouse, France, 2012.

[4] Fletcher, R. W., The next step: a fully integrated global multi-modal security and safety management system. *Proceedings of the 30th International System Safety Conference*, Atlanta, GA, 2012.

[5] Stoneburner, G., Toward a unified security/safety model. *Computer*, pp. 96–97, 2006. https://doi.org/10.1109/mc.2006.283

[6] ABB, Rocky Relationship Between Safety and Security, available at https://www.controlglobal.com/whitepapers/2014/rocky-relationship-between-safety-and-security/ (accessed 3 November 2017).

[7] Hahn, J., Guillen, D.P. & Anderson, T., Process control systems in the chemical industry: safety vs security. *Process Safety Progress,* **25**(1), pp. 40–43, 2006. https://doi.org/10.1002/prs.10114

[8] Dahlstrom, N. & Dekker, S., Security and Safety Synergy – Advancing Security With Human Factors Knowledge. *Wiley Handbook of Science and Technology for Homeland Security*, John Wiley & Sons, Inc, pp. 1–13, 2008.

[9] Pièrre-Cambacédès, L. & Chaudet, C., Disentangling the Relations Between Safety and Security. *Proceedings of the 9th WSEAS International Conference on Applied Informatics and Communications,* Moscow, Russia, pp. 156–161, 2009.

[10] Pietre-Cambacedes, L. & Chaudet, C., The SEMA referential framework: avoiding ambiguities in the terms security and safety. *International Journal of Critical Infrastructure Protection*, **3**(2), pp. 55–66, 2010. https://doi.org/10.1016/j.ijcip.2010.06.003

[11] Baird, P., The Relationship between Safety and Security, available at https://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM559599.pdf (accessed 10 November 2017).

[12] Firesmith, D.G., *Common Concepts Underlying Safety, Security and Survivability Engineering* (Technical Note CMU/SEI-2003-TN-033), Carnegie Mellon University, Pittsburgh, Pennsylvania, 2003.

[13] Hancock, P.A. & Hart, S.G., Defeating terrorism: what can human factors/ergonomics offer? *Ergonomics in Design*, **10(1)**, pp. 6–16, 2002. https://doi.org/10.1177/106480460201000103

[14] Fuller, B.A., Managing transportation safety and security risks. *Chemical Engineering Progress,* pp. 25–29, 2009.

[15] Young, W. & Leveson, N., Inside risks: an integrated approach to safety and security based on systems theory. *Viewpoints: Communications of the ACM*, **57(2)**, pp. 31–35, 2014. https://doi.org/10.1145/2556938

[16] Leveson, N., *Engineering a Safer World: Systems Thinking Applied to Safety.* MIT Press: Cambridge, 2011.

[17] Neiderman, E.C. & Fobes, J.L., A Cognitive Model for X-ray Security Screening: Selection Tests to Identify Applicants Possessing Core Aptitudes, available at http://ntl.bts.gov/lib/20000/20300/20381/PB98125735.pdf (accessed 12 November 2017)

[18] ICAO., *Human Factors in Civil Aviation Security Operations, Doc 9808*. International Civil Aviation Organisation: Montreal, 2002.