Aligning Cyber-Physical System Safety and Security

Giedre Sabaliauskaite and Aditya P. Mathur

Information Systems Technology & Design Pillar

Singapore University of Technology and Design

Singapore

{giedre, aditya_mathur} @ sutd.edu.sg

Abstract

Safety and security are two key properties of Cyber-Physical Systems (CPS). Safety is aimed at protecting the systems from accidental failures in order to avoid hazards, while security is focused on protecting the systems from intentional attacks. They share identical goals – protecting CPS from failing. When aligned within a CPS, safety and security work well together in providing a solid foundation of an invincible CPS, while weak alignment may produce inefficient development and partially-protected systems. The need of such alignment has been recognized by the research community, the industry, as well as the International Society of Automation (ISA), which identified a need of alignment between safety and security standards ISA84 (IEC 61511) and ISA99 (IEC 62443). We propose an approach for aligning CPS safety and security at early development phases by synchronizing safety and security lifecycles based on ISA84 and ISA99 standards. The alignment is achieved by merging safety and security lifecycle phases, and developing an unified model – Failure-Attack-CounTermeasure (FACT) Graph. The FACT graph incorporates safety artefacts (fault trees and safety countermeasures) and security artefacts (attack trees and security countermeasures), and can be used during safety and security alignment analysis, as well as in later CPS development and operation phases, such as verification, validation, monitoring, and periodic safety and security assessment.

Keywords

Cyber-physical systems; CPS; Safety; Security; Alignment; ISA84; IEC 61511; ISA99; IEC 62443; Fault trees; Attack trees.

1 INTRODUCTION

Safety and security are two key properties of Cyber-Physical Systems (CPS) [6, 15]. They share identical goals – protecting CPS from failures [17]. Safety is aimed at protecting the systems from accidental failures in order to avoid hazards, while security is focusing on protecting the systems from intentional attacks. Safety and security are particularly important in industrial control systems, where hazards include explosions, fires, floods, chemical/biochemical spills and releases, potential crashes of vehicles, etc.

In order to protect CPS from failing, safety and security have to be aligned and their 'activities or systems organised so that they match or fit well together' (MacMillan Dictionary's definition of 'align'). When aligned within a cyber-physical system, safety and security work well together in providing a solid foundation of an invincible CPS.

Weak alignment between security and safety may produce inefficient development and partially-protected systems. For example, excess costs could be spent on redundant safety and security countermeasures. Furthermore, security countermeasures may weaken CPS safety, or vice versa – safety countermeasures may weaken security [14]. If there is no alignment between safety and security countermeasures, these interdependencies are not detected in the early system development phases and may lead to a number of problems that affect later CPS development or even operation phases.

Over the years, separate research communities have dealt with threats to security versus safety [16]. Two international standards have been proposed by the International Society of Automation (ISA) to address CPS safety and security needs: ISA84 standard (also called IEC 61511) on safety instrumented systems [5], and ISA99 standard (also called IEC 62443) on control system security [8].

As systems are becoming more complex and integrated, the distinction between safety and security is beginning to weaken. Researchers are starting to recognize a need of collaboration between these two communities [2, 16]. ISA has also identified a need of alignment between safety and security, and formed a working group, Work Group 7 - Safety and Security, to investigate alignment and common issues between security and safety [10].

Some techniques and approaches from the safety domain have already been adapted for security and vice versa. The next step is development of techniques and approaches for integrated improvement of both safety and security [16].

Identifying and characterizing safety and security interdependencies in the early stages of CPS development (specification and design) in order to manage their consequences and optimize operational resources and system performance is still a challenge, which needs to be addressed [14]. Furthermore, the proposed solutions need to be compliant with industrial standards for CPS safety and security.

In this paper, we propose an approach for aligning CPS safety and security lifecycles, based on ISA84 and ISA99 standards. The alignment is achieved by

merging safety and security lifecycle phases and developing an unified model, Failure-Attack-CounTermeasure (FACT) Graph. The FACT graph incorporates safety artefacts (fault trees and safety countermeasures) and security artefacts (attack trees and security countermeasures), and can be used for safety and security alignment analysis.

The proposed approach and the FACT graph not only help to assure that CPS safety (ISA84) and security (ISA99) are implemented in a consistent way, but also enable organizations analyze system vulnerabilities to newly identified accidental and intentional failures during CPS operation, and update countermeasure set in order to provide required level of safety and security.

The remainder of the paper is organized as follows. Section 2 describes the related work. An integrated safety and security lifecycle process is presented in Section 3. Section 4 describes a CPS safety and security alignment model – FACT graph. An example of the FACT graph is presented in Section 5. Finally, Section 6 concludes the paper.

2 RELATED WORK

2.1 CPS Safety

Safety concerns of the process industries can be addressed by the use of the ISA84 standard, which describes the application of Safety Instrumented Systems (SIS) to achieve and/or to maintain a safe state of the process [5]. A SIS is aimed at performing specific control functions to maintain safe operation of the process when predefined conditions are violated [5].

Safety life-cycle consists of the following phases (see Fig. 3.1, left side): Hazard and risk assessment; Allocation of safety functions to protection layers; Safety requirements specification; Design of safety countermeasures; Installation, commissioning and validation; Operation and maintenance; Modification; and Decommissioning [5].

The main objectives of the hazard and risk assessment phase are to determine the hazards and hazardous events of the process and associated equipment, the process risks associated with the hazardous events, and the safety functions to achieve the necessary risk reduction.

In the second phase, safety functions are assigned to protection layers. Then, the required safety instrumented systems and associated safety integrity levels are determined. In the safety requirement specification phase, SIS specific safety requirements are derived from the overall CPS safety requirements, defined during the hazard and risk assessment phase.

In the next phase, safety countermeasure – SIS and other means of risk reduction – are designed taking into account the safety requirements. Then, security countermeasures are implemented, validated, and maintained during the CPS operation.

Typical artefacts, developed/defined throughout safety life-cycle, are the following among others (see Fig. 3.1): failure initiating events, fault trees, safety functions, protection layers, safety requirements and safety countermeasures.

Fault Tree Analysis (FTA) [7] is a technique widely used for hazard and risk assessment. The purpose of the technique is to graphically present the possible normal and faulty events that can cause the top-level undesired event. The fault tree consists of the following components: nodes (undesired events in the system), gates (relations between nodes; can be AND or OR gates), and edges (path of the undesired events through the system).

For the reason that FTA is a graphical technique widely used by researchers and practitioners, we will employ it in our safety-security alignment approach.

In order to illustrate fault tree analysis, we borrowed an example of a pressurized vessel control system from [5]. Pressurized vessel control process is shown in Fig. 2.1, and its fault tree is presented in Fig. 2.2.

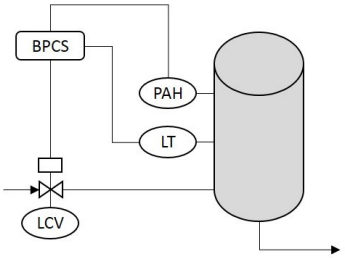

Fig. 2.1. Pressurized vessel process [5].

The process comprises of a pressurized vessel containing volatile flammable liquid [5]. Basic Process Control System (BPCS) is controlling the process by monitoring the signal from the Level Transmitter (LT) and controlling the operation of the Level Control Valve (LCV) (see Fig. 2.1). The system is equipped with a high pressure alarm – Pressure Alarm High (PAH), which is initiated if level transmitter measures high pressure level in order to alert the operator to take appropriate action to stop inflow of material.

A fault tree shown in Fig. 2.2 identifies the events, which contribute to the development of overpressure condition in the vessel [5]. The top event, Overpressurization, is caused either by failure of the basic process control system function, or an external event, such as e.g. fire. BPCS function failure can be caused either by BPCS failure, or field device failures, such as sensor or actuator (valve) failure. Two transfer gates, included into the tree, indicate connections to related fault trees – external event fault tree and BPCS failure fault tree (these trees are not included in this paper).

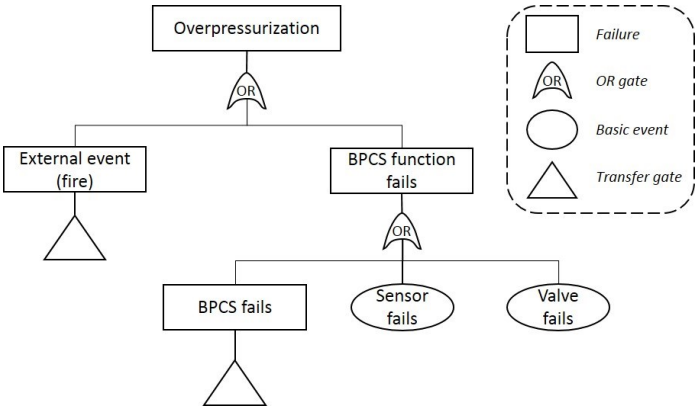

Fig. 2.2. Fault tree of overpressure of the vessel [5].

2.2 CPS Security

To address cyber-physical system security needs, ISA developed an ISA99 standard "Security for Industrial Automation and Control Systems" [8]. The primary goal of this standard is to provide a flexible framework that facilitates addressing CPS vulnerabilities and applying necessary countermeasures in systematic, defensible manner.

ISA99 describes a generic view of an integrated manufacturing or production CPS, expressed as a series of logic levels [8]: Enterprise Business Systems, Operations Management, Supervisory Control, Basic Control, and Physical Process.

In large or complex system it may not be practical or necessary to apply the same security level to all components. ISA99 proposes to divide systems in zones and conduits in order to meet the security goals [8]. Security zone is a logical or physical grouping of physical, informational, and application assets sharing common security requirements. Zones can be formed at different system logical levels, or across levels. Conduits are used to define communications, and may connect entities within zones, or may connect different zones.

Security lifecycle consists of the three main phases: Assessment, Implementation and Maintenance [8]. The assessment phase consists of Process risk assessment, Security requirements specification, Zone and conduit identification, and Risk assessment for each zone and conduit (see Fig. 3.1, right side). During the implementation phase, security countermeasures are designed, validated, developed and verified. Finally, maintenance phase includes operation and maintenance, security monitoring and periodic assessment, and modification and decommissioning.

Typical artefacts, developed/defined throughout security lifecycle process, include the following items among others: attack trees, security requirements, security zones and conduits, and security countermeasures.

Integrity, availability and confidentiality are three high-level cyber security objectives for CPS [9]. A lack of confidentiality results in disclosure, when an unauthorized entity gains access to data. A lack of integrity leads to deception – when an authorized party receives false data and believes it is true. While a lack of availability results in denial of service (DoS) when an authorized entity cannot receive commands or data. Deception, disclosure and DoS are three basic types of cyber-attacks on CPS [9].

Attack trees [3, 11] are widely used for security risk assessment. Attack tree is a graph that describes the steps of attack process. It uses the same basic symbols as fault trees: nodes (represent attacks), gates (AND and OR gates), and edges (path of attacks through the system). Several authors propose to use additional symbols in attack trees. E.g. dynamic, "trigger" edges [12] can be used in situations when one attack event (e.g. Attack 1) triggers the other (e.g. Attack 2). In this case, Attack 2 can be realizable only if Attack 1 has been completed.

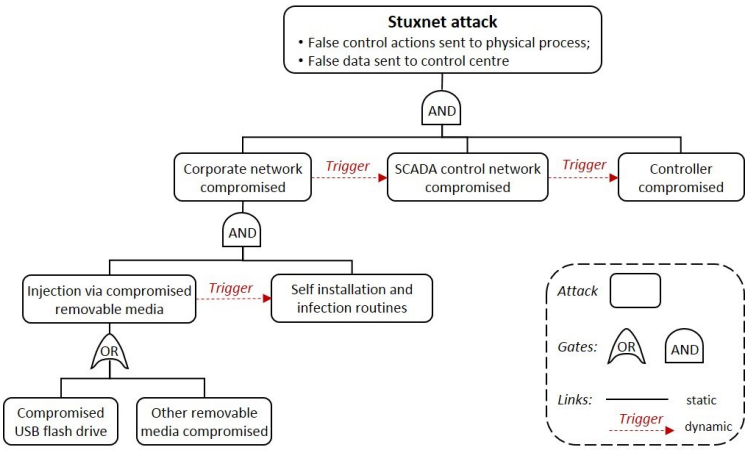

Fig. 2.3. Attack tree example – Stuxnet.

An example of an attack tree is shown in Fig. 2.3. It depicts attack process steps of the Stuxnet attack [1]. The goal of the Stuxnet attack is to compromise controller, which is controlling a SCADA system. The attack starts with injection via compromised removable media, which could be done by user opening a compromised file folder either on USB flash drive, or other removable media. Once this step is completed, Stuxnet worm instantaneously starts its self-installation and infection routines, thus there is a "trigger" line between these nodes. After injection and self-installation and infection routines are completed, an attacker is able to compromise corporate network, which allows him to gain access to SCADA control network, and eventually to compromise a controller.

Several authors proposed to add defense mechanisms to the attack trees [3, 11]. Defense nodes (security countermeasures) can be attached either to attack leafs [11], or to any node in an attack tree, as defined in the Attack Countermeasure Tree (ACT) approach [3]. In an ACT approach, once attack tree is constructed, and possible security countermeasures are attached to the attack nodes, security analysts can select a set of security countermeasures for implementation, considering a given budget [3].

2.3 Safety and Security Integration

Safety and security are interdependent, and these dependencies have to be considered during CPS design phase. There are four types of interdependencies between safety and security [14]: 1) conditional dependencies – security is a condition for safety and vice versa; 2) reinforcement – safety and security countermeasures can strengthen each other; 3) antagonism – they can weaken each other; and 4) independence – no interaction between safety and security.

Several techniques have been proposed in literature for integrating safety and security. They include unified risk definition [2], safety and security life cycle model [17], detecting conflicts between safety and security requirements [13], and integrated graphical model [4] among others.

In [2], authors recommend to expand definition of the safety term hazard to include security related risks. A new definition of mishap is proposed. A mishap is an unplanned event, or series of events, that result in death, injury, occupational illness, or other harm to individual's well-being; damage to or loss of equipment or property; or harm to an organization. These events include system, equipment or component failures, design flaws, user errors, intentional attacks, etc.

A life cycle model for integrated safety and security in automation systems is described in [17]. It focusses on resolving conflicts between safety and security at the requirements and functional levels. Such a life cycle model and its conflict resolution framework are the basis of combining formerly separated networks for safety (e.g. fire alarm system), security (e.g. access control) and operation.

In [13], authors propose a technique for detecting conflicts between safety and security requirements, which helps alleviate contradictory requirements. A tool is used to detect truly coupled requirements among two domains (safety and security), providing system designers with information on requirement contradictions.

In [4], a method for quantitative security risk assessment of complex systems is proposed. It combines fault trees with attack trees by integrating attack trees into pre-existent fault trees. The proposed approach allows considering the interaction of malicious attacks with random failures.

In 2009, ISA formed a joint working group to promote awareness of the impact of cyber-security issues on the safe operation of industrial processes – ISA99

Work Group 7 [10]. To the best of our knowledge, there are no work results published by this group yet.

Despite the existing solutions, there is still a need of an approach, which would help to design safe and secure CPS [14], and which would be compliant with industrial standards for CPS safety and security.

3 INTEGRATED CPS SAFETY AND SECURITY LIFECYCLE PROCESS

We propose a CPS safety and security alignment approach. The alignment is achieved by merging safety and security lifecycle phases and developing a unified model, failure-attack-countermeasure (FACT) graph (see Fig. 3.1).

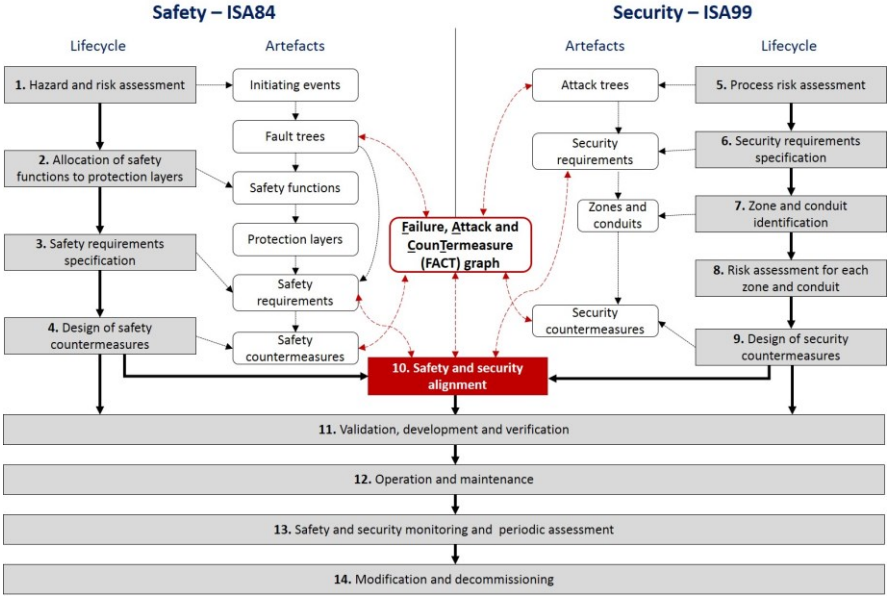

Fig. 3.1. Merged ISA84 and ISA99 lifecycles.

The merged safety and security lifecycle model, which consists of 14 phases, is shown in Fig. 3.1. The process starts with CPS safety risk assessment and design phases (phases 1 – 4), borrowed from ISA84, followed by security risk assessment and design phases (phases 5 – 9), taken from ISA99. In phase 10, the alignment between safety and security is performed. Finally, phases 11-14 are the merged phases of ISA84 and ISA99 lifecycles and include validation, development, and verification, operation and maintenance, safety and security monitoring and periodic assessment, and modification and decommissioning related activities.

The failure-attack-countermeasure (FACT) graph is formed throughout phases 1-9 of the merged safety and security lifecycle. It incorporates various artefacts: safety artefacts (fault trees and safety countermeasures) and security artefacts (attack trees and security countermeasures). This graph is useful not only for evaluating safety and security alignment in phase 10, but also for safety and security verification and validation in phase 11, and for monitoring and periodic assessment in phase 13. The alignment phase (phase 10) and the FACT graph are described in more detail in Section 4.

4 CPS SAFETY AND SECURITY ALIGNMENT USIGN FAILURE-ATTACK-COUNTERMEASURE GRAPH

As it has been mentioned in Section 3, FACT graph is formed throughout phases 1-9 of the merged safety and security lifecycle process. Various artefacts from these phases are used as inputs for the FACT graph as shown in Fig. 4.1: fault trees, safety countermeasures, attack trees, and security countermeasures. Furthermore, security requirements and safety requirements along with FACT graph are the inputs for safety and security alignment analysis.

The FACT graph construction consists of the following four steps:

Step 1. The construction of the graph starts with importing failure trees at the end of the safety hazard and risk assessment phase (phase 1). Whenever possible, interrelated fault trees are connected, using AND or OR gates, in order to provide a complete view of possible failures of the system. These fault trees form a frame of the FACT graph.

Step 2. As soon as the definition and design of safety countermeasures is completed (phase 4), safety countermeasures are added to the FACT graph. They are attached to the failures they are aimed at preventing. This mapping allows us to see the coverage of safety failures by safety countermeasures.

Step 3. Attack trees, formed during process risk assessment phase (phase 5), are added to the FACT graph. Attacks, related to failures in a FACT graph, are attached to the corresponding safety failures. Attack trees are incorporated into fault trees by the use of OR gate, which indicates that a failure may be caused either by accidental failures, or by intentional attacks.

Step 4. After completion of the security countermeasure design phase (phase 9), security countermeasures are added to the FACT graph. We can use ACT technique [3] in this step, which allows attachment of security countermeasures to any node of the attack tree (see Section 2.2).

The FACT graph, constructed during steps 1-4, is a comprehensive system safety and security model, which shows safety and security artefacts and their relationships. It can be used for safety and security alignment analysis (phase 10). In this phase, it is important for safety analysts to work together with security analysts in order to identify any misalignment, duplicates or missing elements. For

this purpose, safety requirements, defined in phase 3, and security requirements, defined in phase 6 of the merged lifecycle, are used (see Fig. 4.1). In phase 10, FACT graph needs to be reviewed and compared against safety and security requirements to determine if the requirements are satisfied, i.e. if proposed safety and security countermeasures provide the necessary risk reduction to achieve tolerable risks of the CPS.

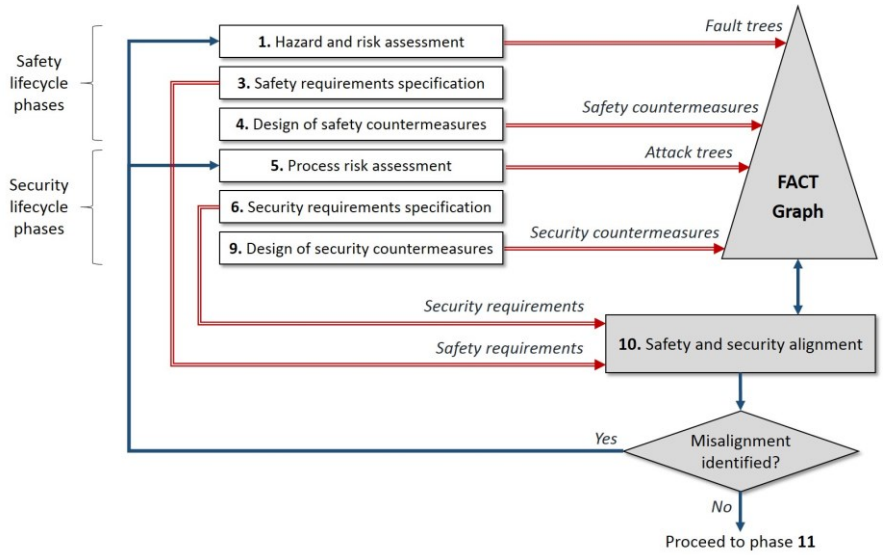

Fig. 4.1. Safety and security alignment process.

Furthermore, FACT graph can be used in later CPS development and maintenance phases as well, e.g. in phase 11 for safety and security verification and validation, and in phase 13 for monitoring and periodic assessment. As new types of failures and attacks are being continuously reported, these newly identified failures and attack should be added to the FACT graph in order to determine if current countermeasure set is sufficient for protecting CPS.

5 FACT GRAPH EXAMPLE

This section includes an example of the FACT graph. The FACT graph construction process comprises of four steps, as defined in Section 4. In the first step, fault trees are imported into the FACT graph and their inter-connections are established. In this example, we will use the fault tree of overpressure of the vessel, borrowed from Fig. 2.2.

In the second step, safety countermeasures are added to the FACT graph. In our example, three safety countermeasures are added, as shown in Fig. 5.1: SAF1 - a

high pressure alarm – Pressure Alarm High (PAH) (see Fig. 2.1), which is activated if level sensor measures high pressure level in order to alert the operator to take appropriate actions to stop inflow of material; SAF2 – redundant sensor, which could be used in a situation when the primary sensor fails; SAF3 – redundant valve, used in a situation when the primary valve fails.

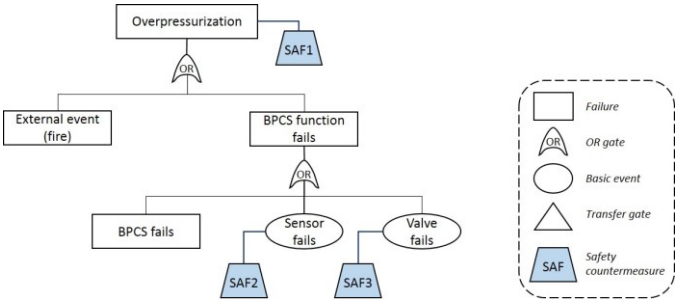

Fig. 5.1. Failure and safety countermeasure graph of overpressure of the vessel.

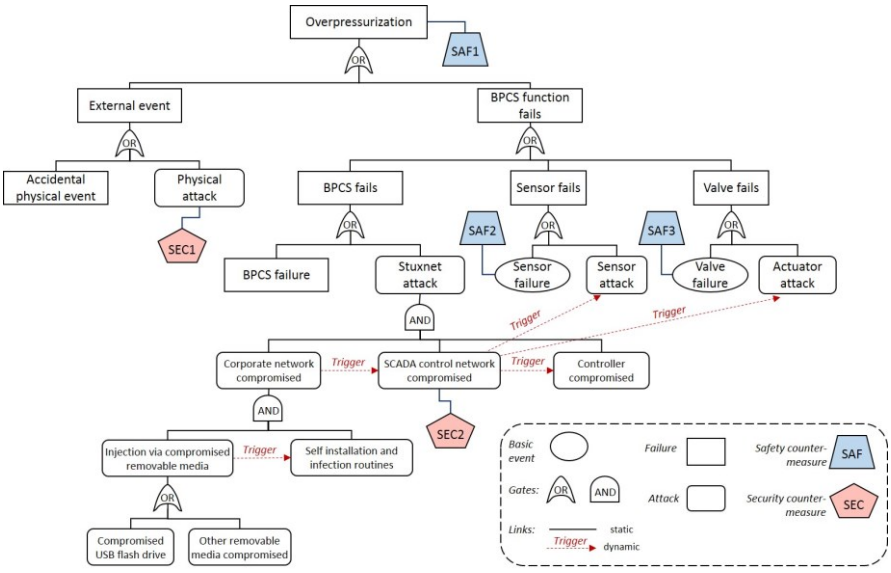

Fig. 5.2. Failure-Attack-Countermeasure (FACT) graph of overpressure of the vessel.

In the third step, attack trees are added to the FACT graph. In our example, Stuxnet attack tree (see Fig. 2.3) is attached to the failure BPCS Fails using OR gate: BPCS may fail accidentally, or it may be caused by a malicious Stuxnet attack. In addition, three more attacks are added to the graph: Physical attack, Sensor Attack, and Actuator attack. It is important to add inter-connection between attacks to the graph as well. In our example, sensor and actuator attacks may be

triggered if SCADA control network is compromised. Thus, links between these attacks are added to the graph (see Fig. 5.2).

Finally, in the fourth step, security countermeasures are added to the graph. Two security countermeasures are added to the vessel overpressure graph (see Fig. 5.2): SEC1 – countermeasures against physical attacks to prevent unauthorized access to the equipment, such as security guards, cameras, locks, etc.; SEC2 – countermeasures for detecting SCADA control network attacks. Detection and mitigation of control network attacks is crucial, because it will prevent not only a Stuxnet attack, but also sensor and actuator attacks. Various intrusion detection techniques can be used for detecting attacks on SCADA control networks.

6 CONCLUSIONS

In this paper we have proposed an approach for aligning cyber-physical system safety and security at early development phases. The proposed approach suggests a way to integrate safety and security lifecycle process phases, defined by ISA84 and ISA99 standards. Using this approach, practitioners may align CPS safety and security activities, by following the merged 14-phase safety and security lifecycle process (see Fig. 3.1), during which alignment model – FACT graph – is created.

The FACT graph can be used to identify any misalignment between safety and security countermeasures, as well as countermeasure duplicates and missing means of protection. In FACT graph, safety and security countermeasure are attached to the relevant faults and attacks, thus it is easy to identify interrelated countermeasures and analyze their interdependencies.

FACT graph is built on a frame of interconnected CPS failures and attacks, and it is continuously updated during CPS development and operation phases by adding newly identified failures and attacks to it. This will help to determine if current countermeasures are sufficient to detect and mitigate newly identified failures and attacks. Furthermore, FACT graph will help to identify redundant safety and security countermeasures – countermeasures, which are aimed at preventing the same attack/failure from happening. Safety and security specialist along with managers will be able to select and optimal countermeasure set to provide necessary protection considering a given budget.

Further research is needed evaluate the proposed approach in a real CPS. We are planning to apply the safety and security alignment approach in an industrial process control system, water purification CPS, which we are currently developing.

Acknowledgments

This research is supported by a start-up grant from the Singapore University of Technology and Design, (http://www.sutd.edu.sg). It is a part of ongoing research at the iTrust – Center for Research in Cyber Security.

7 REFERENCES

[1] S. Karnouskos, “Stuxnet worm impact on industrial cyber-physical system security,” in Proceedings of the 37th IEEE Annual Conference on Ind. Electronics Soc. (IECON 2011), pp. 4490-4494, November 2011, doi:10.1109/IECON.2011.6120048.

[2] G. Stoneburner, "Toward a Unified Security-Safety Model," Computer, vol.39, no.8, pp.96-97, August 2006.

[3] A.Roy, S. K. Dong, and K. S. Trivedi, "Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees," in Proceedings of the 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), pp. 1-12, June 2012.

[4] I. Nai Fovino, M. Masera, and A. De Cian, “Integrating cyber attacks within fault trees,” Reliability Engineering & System Safety, vol. 94, no. 9, pp. 1394-1402, September 2009.

[5] ANSI/ISA 84.00.01-2004, Application of Safety Instrumented Systems for the Process Industries. The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 2004.

[6] L. Piètre-Cambacédès and C. Chaudet, “The SEMA referential framework: Avoiding ambiguities in the terms “security” and “safety”,” International Journal of Critical Infrastructures Protection, vol. 3, no. 2, June 2010.

[7] F. Reichenbach, K.-J. Alme, and J. Endresen, "On the significance of fault tree analysis in practice," in Proceedings of the IEEE Conference on Emerging Technologies & Factory Automation (ETFA 2009), pp. 1-7, 22-25 September 2009.

[8] ANSI/ISA-99-00-01-2007. Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models. The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 2007.

[9] S. Amin, “On Cyber Security for Networked Control Systems,” PhD Thesis, University of California, Berkeley, 2011.

[10] ISA 99 Work Group 7 – Safety and Security (Joint with ISA84 committee). http://isa99.isa.org/ISA99%20Wiki/WG7.aspx (references on 11 April 2014)

[11] C.-W. Ten, C.-C. Liu, and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," Power Engineering Society General Meeting, pp. 1-8, June 2007, doi: 10.1109/PES.2007.385876.

[12] S. Kriaa, M. Bouissou, and L. Pietre-Cambacedes, "Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments," in Proceedings of the 7th International Conference on Risk and Security of Internet and Systems (CRiSIS 2012), pp. 1-8, October 2012, doi: 10.1109/CRISIS.2012.6378942.

[13] M. Sun, S. Mohan, L. Sha, and C. A. Gunter, “Addressing Safety and Security Contradictions in Cyber-Physical Systems”, in Proceedings of the Workshop on Future Directions in Cyber-Physical Systems, July 2009.

[14] L. Piètre-Cambacédès, and M. Bouissou, "Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes)," in Proceedings of the IEEE International Conference on Systems Man and Cybernetics (SMC 2010), pp. 2852-2861, October 2010.

[15] A. Banerjee, K.K. Venkatasubramanian, T. Mukherjee, S. K S Gupta, "Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems," in Proceedings of the IEEE , vol.100, no.1, pp. 283-299, January 2012.

[16] L. Piètre-Cambacédès and M. Bouissou, “Cross-fertilization between safety and security engineering,” Reliability Engineering & System Safety, pp. 110-126, February 2013.

[17] T. Novak and A. Treytl, "Functional safety and system security in automation systems - a life cycle model," in Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2008), pp. 311-318, September 2008.