FIA

Strategic Research into Safety and Security for the Automation Industry

WP3 - Deliverable D3.2 (Guideline for Companies)

Contributors: MDH, SICS, Volvo CE, Boliden and Safety Integrity
Editor: Kaj Hänninen, Mälardalen University, Sweden
Deliverable D3.2 (Guidelines for Companies)

Introduction
This guideline is compiled from the deliverables in the FIA-PiiA project that was executed in 2015. The guide will exemplify how functional safety activities can be extended to include parts of IT-Security. This guideline should be read in conjunction with Appendix A and deliverables D1.1, D1.2. The deliverables describe the reasoning behind the recommendations in this guide.

Including IT-Security as a natural part of safety development is important to address potential risks that modern interconnected systems and equipment introduce. Many of the products that we use on daily basis are connected to public or semi-public networks. The interconnection of devices introduces new type of security risks that may affect the safety of the system, thus it is recommended that an extended risk identification, assessment and management procedure should be included as part of the safety work.

Note that this guideline exemplifies a one-way approach. This implies that the safety work is extended to include security, it does however not imply that the security work is extended to cover functional safety. A one-way approach is a natural start before a full harmonisation of the safety and security disciplines is performed. Moreover, the guide is based on the requirements from two widely used standards, the ISA/IEC-62443, “Industrial communication networks — Network and system security” and IEC/EN 62061, "Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems” See deliverable D1.2(A method for joint assessment and trade-offs for safety and security) for information about the requirements and the standards.

Background
As of today, safety assurance and certification of safety critical systems has mainly focused on the safety aspect of systems. The increasing interconnection of devices through different type of networks imposes new challenges that have not received enough attention in safety domain. The primary challenge is to address security in combination with safety. Safety and security are not just complementary but also, to a high degree, interdependent in that security issues may affect safety and vice versa. In general, safety and security are two separate disciplines, governed by completely different standards. They do however have the same aim, to reduce the systems risks that may cause harm. Experiments and research has shown that modern systems can be exposed to surprisingly simple security flaws giving an attacker the control of the safety related functionalities. This has however not yet resulted in approaches to address safety and security in combination, even though a combined approach is imperative to reduce the overall risks to acceptable levels. There is currently very little knowledge on how to jointly assure safety and security in development. A number of recent project has however address safety and security in combination. For example, the on-going Healing Vulnerabilities to Enhance Software Security and Safety (HEAVENS project 2013 - 2016) [2] is focusing on identifying security
vulnerabilities and providing methodologies (and tools) for security testing of safety critical software in the automotive domain. The main aim of the project is to facilitate vulnerability identification and requirements specifications to mitigate security risks and their impact on safety. The on-going Safety and Security Modelling project (SESAMO 2012-2015) [3] focus on both safety and security aspects of systems, with the aim to provide component based design means to jointly address safety and security issues in development. In addition, the project expects to provide procedures for integrated analysis of the properties for different domains such as avionics, transports and industrial control. The finished SSpiia project (2013 - 2014) [4] investigated the requirements for the process-industrial IT and automation domain to identify the feasibility and benefits of introducing composable safety-certification and platform security in virtualized systems.

Functional Safety and IT-Security

Harmonising the safety and security work in development is not a trivial task. The disciplines are typically governed by separate standard that advocate different approaches to reduce the risks with the systems.

Some commonly used functional safety and IT-security standards include:

- **Functional safety**
  - IEC 61508 Generic E/E/PE systems
  - US RTCA DO-178C Avionics
  - US RTCA DO-254 Avionics
  - IEC 62304 - Medical
  - IEC 61513, Nuclear
  - IEC 61511-x, Process industry
  - IEC 62061 and ISO 13849-x Machinery
  - EN 5012x, Railway
  - ISO 25119 - Agriculture and Forestry
  - ISO 26262 - Road Vehicles

- **IT-Security (also called cyber security)**
  - ISO/IEC 2700x Information management
  - NERC 1300 Infrastructure
  - ISO 15408 Common criteria
  - ISA 99 Automation and control
  - IEC 62443-x-x Automation and control

It is obvious that combining the requirements from standards require a large amount of work to achieve any harmonisation that is both efficient and beneficial from assessment and certification views. A more feasible approach is to include only the necessary parts of security work in the safety lifecycle, i.e., activities that assure that the security risks affecting safety are

---

1 In the sense that the assurance work can be utilised as assessment argumentation in both disciplines
identified, assessed and managed in some way. To achieve this, we propose that the safety organisations apply the following in the safety work.

**Prop. 1 - Assessing and extending the System Definition**

The system definition used in the ordinary safety work should be assessed against potential security vulnerabilities and threats. The definition is imperative in that it defines the scope of risk reasoning. The risk analysis is thus only valid for the specific system definition. This implies that whenever a system definition (or the constituents of the definition) change, the risk analysis may be affected (new risks may be introduced and existing ones may be affected). In general, a system definition shall cover the system, the environment and the entire scope of the systems including the interfaces to the environment and within the system. For proper consideration of security issues, this definition must however be extended to include the organisation, the physical or cyber assets that affect operations (see deliverable D1.2 for detailed information).

Since all hazards originate from within a correct and complete system definition (this is a basic prerequisite that must hold when reasoning about risks) the organisation need to evaluate if the security threats can affect the system or the constituents of the system, that is, as a first step they need to investigate if security threats can exploit (discover, execute, access, change, modify etc.) any vulnerabilities in i) the product itself, ii) the environment (the physical and organisational), iii) the interfaces (within the product and between the product and the environment as well as cyber assets affecting the product or operations) or iv) the scope of the system definition.

The product itself contains all the item(s) that delivers the intended functionality. The environment is the area where the product is developed, tested, operated, maintained etc. The interfaces between the product and the environment are the points and areas where the product interacts (or interferes) with the environment (and vice versa) as well as the cyber assets affecting the product or operations. The scope of the definition is everything included in reasoning about safety and security, i.e., the scope shall cover the product, the environment, the interfaces and anything that could potentially affect any of them. Note that the scope of reasoning may well be larger and cover more than the product, environment and interfaces altogether. In defining the boundaries of the product, the interfaces and the environment, potential threats and vulnerabilities must be accounted for. The origins of threats and vulnerabilities may well affect boundaries of the product, the interfaces, the environment and the scope of reasoning.

**Prop. 2 - Extending hazard analysis to cover security threats**

---

2 Basically, everything that interface or affect the development or operation, e.g., people (design authorities, subcontractors etc.), fieldbuses and I/O for system functionality, internal product buses and interfaces, sensors, actuators, configuration interfaces, control, monitoring and diagnostics interfaces, maintenance, testing and upgrading interfaces, infotainment interfaces, external product interfaces (e.g., authentication and authorization interfaces, session management interfaces, USB interfaces, ...), cellular interfaces and additional assets such as., mobile-enabled devices, printers, USB devices, computers,...
When including security threats as potential sources of hazards, additional and previously unforeseen hazards may be identified (see deliverable D1.1 for an example). One of the main reasons for this is the fact that the scope of reasoning is extended and that intentional- and accidental misuse of the constituents of the system definition (i.e., the product, the interfaces etc.) must be accounted for. Thus it is strongly recommended that the hazards identification process apply the new system definition (as explained in the section above) and that the process either 1) assures that the safety personnel have the required level of knowledge of security, or 2) includes personnel with security knowledge.

Note that the process of identifying hazards differ slightly between the safety and security disciplines. In the security discipline potential threats and vulnerabilities are identified. These may then be the sources of different hazards. Whereas in the safety area, the hazards are sometimes identified without any specific consideration of the sources. The sources (or causes) are identified later and mitigations are defined based on the risk classification and the sources of the hazards. Thus a harmonised hazards identification process is likely to be more extensive when both safety and security are accounted for.

In general, the hazards identification process for an extended safety approach that include security risks shall consider harm to people, damage to the environment and significant financial losses for businesses. The reasoning about hazards should include the possible security threats that can affect safety (see an example of threats in Appendix A). In identifying hazards the process must be extended, 1) to include both intentional misuse and accidental misuse 2) with reasoning about threats that are aware of the consequences (i.e., threats using the system as intended or intentional misuse or accidental misuse, 3) with reasoning about threats that are unaware of the consequences (i.e., threats that may intentionally or unintentionally exploit a vulnerability by using the system as intended or as unintended). This gives the following cases to consider:

- Cases when a threat knows that it is aware of the consequences
- Cases when a threat don’t know that it is aware of the consequences
- Cases when a threat knows that it is unaware of the consequences
- Cases when a threat don’t know that it is unaware of the consequences

The above hazards identification process may at first glance seem as a reverse engineering process (or bottom up approach) in the sense that vulnerabilities and threats are identified, and based on that, the potential hazards identified. However, the original hazards analysis process applied in the safety area should still be applied but extended with vulnerability and threat models applied in the security domain. This results in a process where hazards are identified both with and without knowledge of the threats, thus it will be a combination of both a top-down and bottom-up approach. This will result in a more complete hazards identification process that has the potential to increase safety and to reduce the number of undetected risks due to security issues.
Prop. 3 - Classifying risks - Including security risks that affect safety

When including security in the risk identification process the number of potential hazard may increase, and the risk classification of already identified hazards may have to be re-assessed (see deliverable D1.1 for more information). Both new hazards and existing hazards that have been identified must be re-classified since security threats may introduce new hazards and affect the existing ones.

In applying IEC 62061 [1], the hazards identified shall be classified by considering the consequence of each hazard, the severity (S) of each hazard, the rate (F) of occurrence, the occurrence probability (P) of each hazard and measures for hazard avoidance (A). In classification of hazards the Severity (S) shall be defined by the consequence. Thus the fact that security is included in the classification process does not affect the basis of the classification procedure itself. In fact, when classifying safety risks, the risks originating from security breaches shall be classified in the same way as those originating from safety breaches. This will result in a generic classification procedure applicable for both safety and security risks (note that in doing this the mitigations for security breaches must follow the recommended techniques and methods outlined in the safety standard).

The severity level and the sum of the Frequency, Probability and Avoidance may, then determine the class, and safety integrity level.

Prop. 4 - Reducing risks - Defining mitigations

It is advisable that the risk reduction process distinguishes between:
1. Hazards originating from a pure safety approach
2. Hazards that originate from security threats and affect safety
3. Hazards that originate from a combination of both a safety issue and a security issue

The main reason why the origins (causes) of the hazards should be categorised is the fact that the risk reduction measure then can be more appropriately designed.

For case #1 where the origins of the hazards are purely safety related (e.g., due to malfunctions, foreseeable misuse etc.) the risk reduction measures, techniques and recommendations in IEC/EN 62061 may be followed.

For case #2 and #3 the risk reduction process need to consider if the risk can be reduced according to 1) the safety standard or 2) to the security standard(s) 3) with a combination of both safety and security standards (note however that the recommended practices outlined in the safety standard must be followed in both cases).
To determine which reduction measures that are the most appropriate ones, the causes of the hazards must be identified. This information can usually be found in the hazard analysis log, FMEAs and in other type of analyses (e.g., FTA, ETA etc). The risk reduction process then have to decide upon reduction measures. The key here is to address the hazards to 1) eliminate the hazard by preventing the cause(s) or avoiding the consequence(s) or 2) reduce the occurrence of the hazards or 3) control the hazards. This can only be achieved by an understanding of the hazards causes, consequences and frequencies.

**Prop.5 - Defining new roles, responsibilities and accountabilities**

Extending safety work to cover security aspects require roles, responsibilities and accountability to be defined for the work. In some standards the roles and responsibilities are outlined in detail whereas in other standards they are not. The proposed joint approach requires that all persons involved in the work know their roles and responsibilities. This is imperative to 1) assure the required degree of independence between roles and 2) to assure that responsibilities for the roles are adequate to cover the extended safety scope. To achieve this the typical roles and responsibilities in the safety work need to be revised and possibly extended (e.g., Designer roles, with responsibilities to assure that security has been addressed in the safety work).
References


