A Security Engineering Process Approach for the Future Development of Complex Aircraft Cabin Systems

Hartmut Hintze, Benjamin Wiegraefe, and Ralf God

TUHH, Institute of Aircraft Cabin Systems, Hamburg, Germany
{hartmut.hintze,benjamin.wiegraefe,ralf.god}@tuhh.de

Abstract. Due to increasing functionality associated with rising complexity of aircraft cabin systems which are used by cabin crew, passengers, maintenance staff and other stakeholders, security engineering has to become an integral part of the system engineering process in aviation industry. This paper deals with a security engineering process approach for the development of complex aircraft systems, which is fully integrated into the development process. As an appropriate process model we introduce the so called three-V-model, which represents the governing system engineering process (SEP) associated with the safety engineering process (SafEP) and the security engineering process (SecEP). All three processes are pursued concurrently and are interacting reciprocally on each development level with the predominant SEP. We describe in detail involved security engineering activities and finally demonstrate how the interaction between the SEP and the SecEP is improved and optimized by the use of so called security context parameters (SCPs).

Keywords: Security, Aircraft Cabin Systems, Complex Systems, Development Process, Three-V-Model, Security Context Parameters.

1 Introduction

The cabin management system takes on a central role for all tasks to operate the aircraft cabin. Primary functions are communication, indication, control, monitoring and configuration of other cabin systems. For this reason it represents a complex system characterized by a large amount of interactions between a plurality of aircraft cabin systems. To achieve the objectives of SAE ARP-4754 [1] for certification of highly integrated and complex aircraft systems, the development process is following a process model which is called the V-model. The development of the system functions is supported by the safety assessment process [1-2], which follows a V-model as well and has to ensure the reliability of the system functions. The combination of the functional V-model and the safety V-model is known in literature as the Two-V-Model [3]. To cover security requirements which are related to the system functions, the recent EUROCAE / RTCA documents [4] provides guidance material for a security engineering process. This process will become mandatory for the development of aircraft cabin functions and related systems. In this paper we take up this approach, refine it and integrate it as a 'third V' to end up with an appropriate and

L.J. Janczewski, H.B. Wolfe, and S. Shenoi (Eds.): SEC 2013, IFIP AICT 405, pp. 190–202, 2013.

comprehensive new process model for the development process in aircraft industry. The resulting Three-V-Model is intended to be used as the baseline for the development of future aircraft cabin systems and will consider the system engineering process (SEP) associated with the safety engineering process (SafEP) and the security engineering process (SecEP) at the same time. Furthermore the interactions between the SEP and the SecEP are improved via the introduction of so called security context parameters (SCPs). Theses parameters help to quantify and transfer required information for security management from the SEP to the SecEP and vice versa. This approach avoids time consuming information filtering work at SecEP side and thus provides the opportunity for speeding up the overall development process.

2 System Security in the Development of Cabin Management Systems

2.1 Historical Overview

Within the past 20th century engineering work in commercial aviation was focused on improving the performance parameters for higher payload, extended range, higher speed and more comfort for the passengers. Important milestones were reached by major achievements in aircraft design, engine technology and by the use of pressurized cabins for higher cruise altitude.

The use of electronics within passenger aircraft started with engine control in the 1950s and then in the 1970s was extended to electronic flight control. A peak was reached in 1988 when Airbus introduced its fully digital fly-by-wire technology in the A320. With this aircraft, Airbus completely discarded the use of analog primary flight controls and replaced them by fully computer-controlled digital signaling via an avionics data communication network to control hydraulic actuators at the flight-control surfaces.

Today, in the 21st century the focus has moved to the aircraft cabin with its complex systems. The cabin is the central element within air travel and the business card of the airline. The primary transport service of an airline comes along with a fierce competition for customers and forces the airline to deal intensively with passenger's future travel requirements. The cabin management system with its various service functionalities plays a central role in this struggle for customer satisfaction. Electronics and data network of the cabin management system have continuously been refined over the past 25 years. This on-going evolution led to a mature and sophisticated system. However a still increasing range of cabin functions, maintenance tasks and passenger services and a related growing amount of processes are now culminating in a challenging situation where the existing architecture needs to be reconsidered and reworked in terms of flexibility and scalability to be fit for the future.

Preferred types of architectures for next-generation cabin management systems are based on the concept of distributed systems with wireless communication links e.g. for ad-hoc-sensor networks, mobile PCs and other mobile devices to satisfy the needs of the various stakeholders in the cabin [5-6]. These novel architecture principles

aboard passenger aircraft place special emphasis on the aspects of security. In the past, security was mostly handled by physical security mechanisms: the hardware was physically separated, software was encapsulated and communication paths were regulated and secured. But for distributed architectures with wireless communication interfaces the means of physical security mechanism is no longer sufficient. Hence, it is necessary to establish logical security mechanisms, i.e. security mechanisms against unauthorized access to communication networks, software, information and data of a system. Furthermore, the unauthorized execution of activities within the system has to be prohibited. Logical security in aircraft is becoming more and more a challenge and therefore has to be considered from the very beginning when developing a new aircraft.

2.2 The Need for a Change

A closer look into today's cabin management systems proves that an evolutionary system extension led to the involvement of new stakeholders, an integration of a multitude of functionalities to deal with novel use cases and to an extension of data intercommunication to infrastructures outside of the cabin as described in [6]. This progression was mainly achieved on a system level and thus can be considered to be a bottom-up approach in the development process. In consequence the emerging security issues were predominately handled on a system level as well. This strategy has led to a substantial workload dealing with security at a late engineering stage during the overall aircraft development process. According to systems engineering principles [7] it is feared that this strategy can negatively influence development timelines and development cost and may even lead to imperfect or unsatisfying technical solutions.

To cope with these potentially adverse effects there is the need for a change in the development strategy which relocates a significant part of security engineering activities to the first development level, i.e. the aircraft level, and thus enables a favored top-down approach. This top-down approach for security management is feasible when an optimized and standardized communication starts already on an aircraft development level. Further refinement on subsequent development levels will then be reached with reduced effort and in a more directed manner.

Such type of top-down approach for a security engineering process is generally applicable, e.g. in automotive and railway industry or for nuclear power plants and electric power utilities. Due to our specific work in aircraft industry and security, we have tailored this approach to the development of a next-generation cabin management system. The above mentioned means of logical security coming along with novel system architectures in the cabin will be considered.

2.3 The Three-V-Model

Figure 1 shows our so called Three-V-Model. The first V represents the fundamental system engineering process (SEP) for the development of aircraft functions according to literature [1]. The two branches of this V are symbolizing the three major

phases of system design, implementation and system integration. The second V accompanies and supports the basic SEP and represents the safety engineering process (SafEP). This process is well known from literature [2] and focuses on system safety requirements and airworthiness design, i.e. reliability and fault tolerance topics.

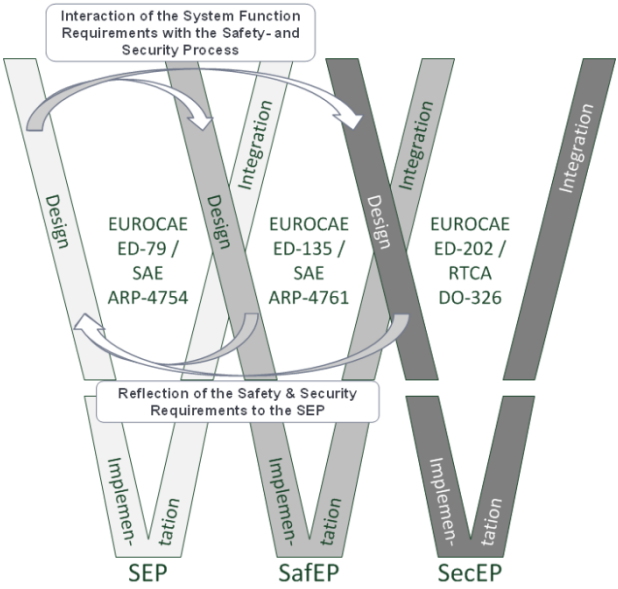

Fig. 1. The Three-V-Model derived from EUROCAE, SAE and RTCA guidelines [1-2, 4] for the systems engineering process (SEP), the safety engineering process (SafEP) and the security engineering process (SecEP)

To make sure that for novel aircraft system architectures the security requirements are visualized and encountered more comprehensively and at an early stage during the development process we introduce an accompanying and supporting third V, which represents the security engineering process (SecEP). A generic specification for a SecEP is given in [4]. To cope with all particular guidelines of the aircraft development process we further on refer to this Three-V-Model as a comprehensive process model. In this model the SEP for the development of system functions, the SafEP covering system reliability and the SecEP to protect the system from attack and misuse are pursued in a concurrent way.

Figure 1 additionally illustrates, that the requirements for the system functions in the SEP are governing the respective safety and security requirements and these requirements reciprocally affect the system functions. The Three-V-Model ensures that for the design of future cabin management architectures the security aspects are encountered right from the beginning. This will guarantee that the required security level (SL) can be finally reached and security can serve as an enabler for the intended system functions.

2.4 The Aircraft Domain Model

Within the well-established safety engineering process (SafEP), i.e. the 'second V', the so called design assurance level (DAL) is defined at an early stage during the development phase. The DAL is introduced by the EASA and FAA documents CS 25.1309 and FAR Part 25.1309 [8] and specifies the relationship between the likelihood that a system functions fails and the respective consequences for the aircraft within its mission. Accordingly, the total loss of the aircraft must be extremely improbable whereas some slight inconvenience to occupants, e.g. the loss of in-flight entertainment, can be tolerated.

By analogy with the DAL definition, the security development process (SecEP) is using a security level (SL), which is currently related to a specific categorization of aircraft cabin functions. In detail this classification is derived from the so called domain model of the aircraft network. This domain model is shown in Figure 2.

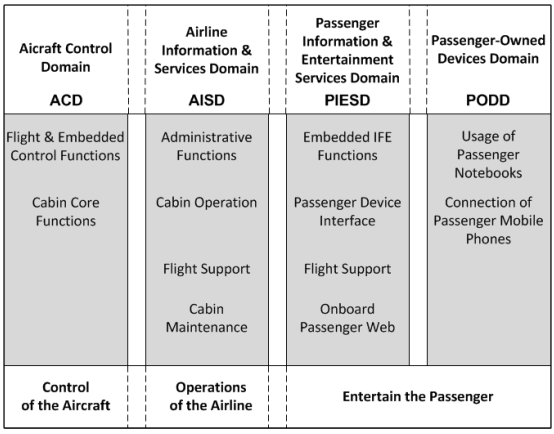

Fig. 2. The aircraft domain model

The domain model of the global aircraft network architecture which is specified by the ARINC report 664P5 [9] comprises four different domains and is depicted in Figure 2. The ARINC report 811 [10] refers to these four aircraft domains for a classification of security domains. The first domain, the aircraft control domain (ACD), represents the highest criticality level and hosts all flight relevant and embedded control functions. Furthermore, basic cabin safety functions are located within the ACD as well. The airline information and services domain (AISD) contains all global functions for cabin operation and maintenance purposes which are not safety critical. This implies that the AISD has a lower SL than the ACD. An even lower SL is assigned to the passenger information and entertainment services domain (PIESD) with its adjacent passenger owned devices domain (PODD) at lowest SL. These two domains host information and entertainment functions and deliver interfaces to connect passenger notebooks or other mobile devices to the aircraft.

However it must be taken into account that a sustainable and more generic approach for a security engineering process must be applicable to all existing and

prospective cabin functions and nevertheless should be in accordance with the nowadays defined domain allocation. Therefore a top-down approach for the security management process which matches with the conventions of the past and allows an efficient handling of challenges in the future has to be ensured. The next chapter describes such type of a top-down approach, i.e. a generic security engineering process.

3 A Generic Security Engineering Process Approach

There are three major objectives for a generic and efficient security engineering process in aircraft development. The first is a top-down approach, i.e. security engineering has to start at the very beginning of the development and to follow the overall process. The second is a global applicability to existing and prospectively expected aircraft functions and the third is an enhanced communication between engineering departments by using a standardized information transfer for security topics on all development levels. The subsequent four sections will provide an elucidation of an approach which is able to comply with these three major objectives:

1. Execute SEP and SecEP concurrently and on all development levels
2. Define the links for process interaction and synchronization
3. Specify the SecEP objectives at a particular development level
4. Use security context parameters (SCPs) for standardized communication

3.1 Execute SEP and SecEP Concurrently and on All Development Levels

The Three-V-Model in Figure 1 suggests three concurrent processes during system development, i.e. the system engineering process (SEP), the safety engineering process (SafEP) and the security engineering process (SecEP). The SafEP and the SecEP are interacting reciprocally with the governing SEP. Figure 3 provides a more detailed view to dedicated development levels.

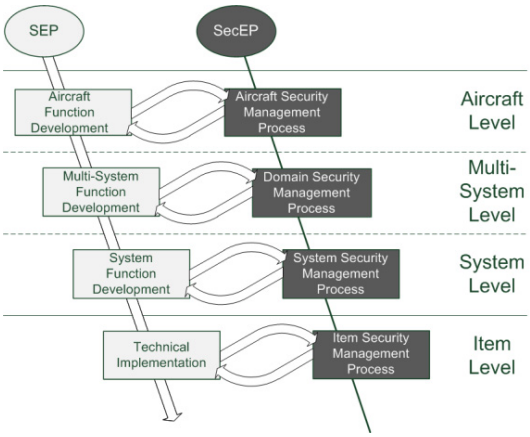

Fig. 3. Development levels of SEP and SecEP and interactions during the design phase

The illustration focuses on the simultaneous execution of the SEP and the SecEP during the functional development of the system, i.e. the system design phase which is represented by the left branch of the V-model. Note, that the established SafEP will not be considered hereafter.

Due to the high complexity of aircraft, the design phase is subdivided into four development levels (cf. Figure 3): the aircraft level, the multi-system level, the system level and finally the item level. Each development level refines the higher level information to an appropriate granularity until the design process reaches the lowest development level, which is the item level. The aircraft level, system level and the item level are defined and described in [1]. The inserted multi-system level is deduced from EUROCAE ED-202 [4], which proposes a security management process for all development levels and points out the need to additionally consider the aircraft domain model (cf. section 2.4) for the risk management within the SecEP. This prerequisite can be referred to a treatment on a multi-system development level. Unfortunately the SEP, as it is today, does not address a multi-system development level. This is due to the fact that still today aircraft functions are grouped and developed hierarchically according to historically defined ATA chapters [11] which do not sufficiently consider system interactions and crosscutting aircraft functions. Hence we have introduced and inserted an implied multi-system level between the aircraft level and system level to consider the aircraft domain model.

3.2 Define the Links for Process Interaction and Synchronization

In order to perform security management within the SecEP the current proposal in EOROCAE and SAE documents [2] is to have an information transfer from the established SafEP to the prospective SecEP. In contrast to this proposal we advocate a direct information link in-between the leading SEP and the parallel and equal SecEP. This is because the complexity of future aircraft systems with progressive logical security considerations requires a security management process, which is no longer a derived subset of the SafEP, but has to be an autonomously executed process and thus has to have direct links to the governing SEP. These links interlace the SecEP and the SEP by peer-to-peer interaction. This finally leads to a concurrent and continuously interacting process flow which is schematically shown in Figure 4.

In line with both, the guidelines for the SecEP [4] and the ISO27005 information technology framework for security techniques and information security management systems [12] Figure 4 provides a more detailed view on aircraft level to the synchronization of the SEP and SecEP. Harmonization of [12] and [4] is ensured, because the latter one only claims the need for a global security management process and [12] explicitly expresses required SecEP activities and covers them in detail. The ISO 27005 framework [12] defines the following required activities: concept establishment, risk assessment, risk treatment and risk acceptance. The risk assessment is further split into risk identification, risk estimation and risk evaluation as per definition of [12].

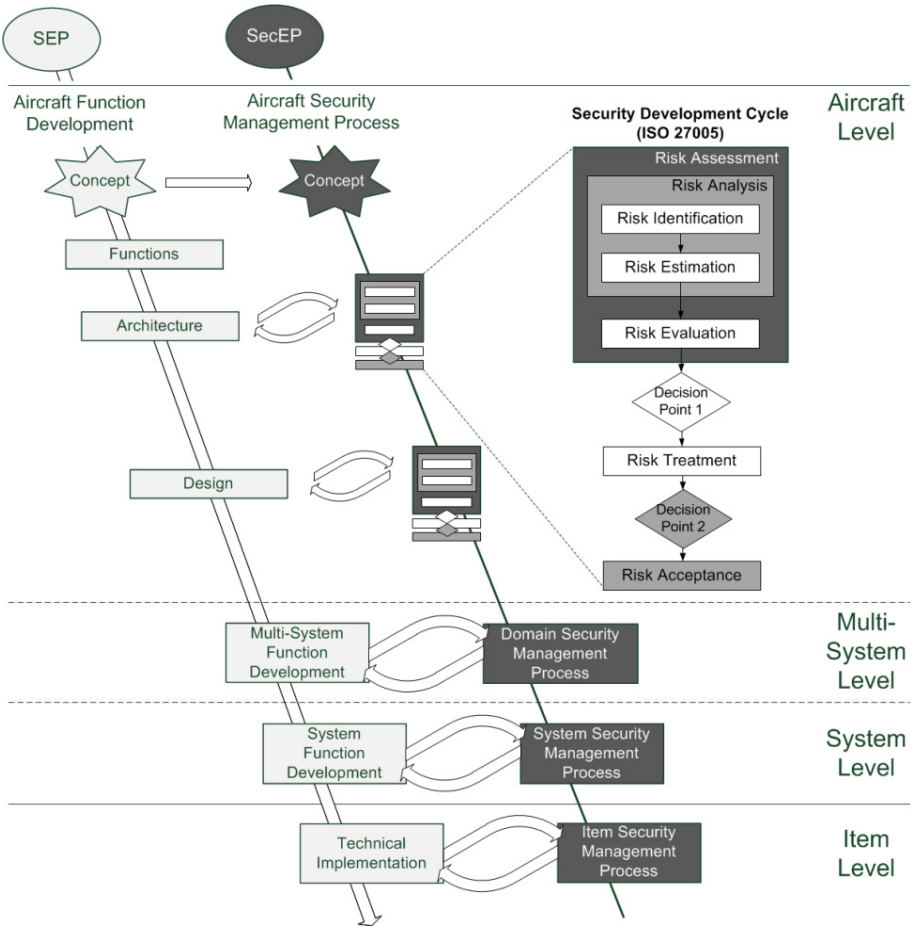

Fig. 4. Particularized SecEP activities at aircraft level interacting with the governing SEP

A comparable refinement of the SEP activities on aircraft level can be deduced from the system development lifecycle according to [1] which defines the four development phases of concept, functions, architecture and design. During concept phase the SEP gathers general and supportive information which is prerequisite for the development of an aircraft. This information might be the operational environment of the considered aircraft including stakeholders, requirements and experience from the development of aircraft in the past. On the next stage follows the elicitation of functions by using the information acquired during the concept phase. During the subsequent architecture phase, the defined functions together with functional requirements are then used to draft the architecture, which assigns the interaction of all pre-defined stakeholders and functions. The subsequent design phase may particularize the proposed architecture, e.g. by a further refinement of functions and assigned stakeholders. However depending on a specific development level the realization of a design phase is optional.

Now it is possible to interlink and synchronize the SecEP with the SEP at defined interaction points. This interlink stipulates the required information exchange which is necessary for the SecEP to be able to perform its activities during the security development cycle. The output of the SEP concept phase is directed to the SecEP concept activity, for establishing all process supporting information. A feedback to the SEP is not required because the output of the SecEP concept is mainly security relevant policies and guidelines. The architecture phase and design phase are linked to the security development cycle as given by the ISO 27005 framework [12]. The latter one enquires SEP information details and therefore specifies the content of the information which has to be exchanged.

The intensity of the performed activities during the security development cycle will differ at specific development levels depending on the SEP derived information details and drive the objectives of the SecEP at a particular development level.

3.3 Specify the SecEP Objectives at a Particular Development Level

A fundamental principle of the V-model is the continuous elaboration of details during the design phase. Engineering information is continuously refined on a dedicated development level. In aircraft development this means that on the initial aircraft level there is predominantly notional information, i.e. abstract data without reference to any technical solution. The aircraft level basically specifies functional groups. Hence, the objectives for the SecEP at aircraft level are an investigation on the consequences and on the probability of the loss of functional groups, i.e. the scope or impact of a loss and the likelihood that an attack is successful and will cause such loss. The impact can be assessed via flight safety relevant and commercial aspects of an investigated functional group. This is similar to activities within the SafEP [13] and thus can be parallelized. The likelihood can be assessed via known communication paths and their classification into communication partners, communication type and direction.

The multi-system level refines the functional groups (e.g. lighting) into generalized aircraft functions (e.g. cabin lighting, emergency lighting and exterior lighting) and allocates them within the aircraft domain model. Thus, major objectives on multi-system level are an impact analysis of the loss of generalized functions on multi-system level, an estimation of the likelihood of an attack, an assignment of attack paths and a security domain allocation. Again the impact can be assessed via flight safety relevant and commercial aspects of a generalized function. On multi-system level the likelihood can be assessed via a known communication partner, a communication direction, the type of information and the purpose of received information. The assessment of these parameters provides additional information on a possible attack path and enables the allocation within the aircraft domain model.

The definition of objectives on an aircraft and multi-system level leads directly to a consistent top-down approach, which can be seamlessly used as a superstructure for nowadays performed security activities on the system level. This generic SecEP approach provides the advantage of filtering out non-security relevant function groups and generalized functions at earlier development levels. This avoids costly and

time-consuming work on later development levels, e.g. the system level. The subsequent section will show how a straightforward and standardized exchange of pre-defined information in-between SEP and SecEP can be achieved by introducing security context parameters (SCPs).

3.4 Use Security Context Parameters (SCPs) for Standardized Communication

The security context parameters are introduced to extract the beforehand identified security relevant information from the SEP in a standardized and simple way. Keeping it short and simple is beneficial, because the system designer in the SEP usually has less knowledge about security management issues and therefore needs to be guided and supported by experts from the SecEP. Standardization can be accomplished by implementing and using predefined security context parameters (SCPs) comprised of parameter types and valid values. Due to a specific level of detail during aircraft development, the parameter types and values are dependent on a specific development level. Parameter types and values representing the aircraft level are given in Table 1.

Table 1. Security context parameters (SCPs) on aircraft development level

Parameter Type	Valid Values
Function Group Name	[aircraft function group name]
Communication Partner	[stakeholder, aircraft function group]
Communication Direction	[bidirectional, unidirectional (send), unidirectional (receive)]
Type of Communication	[variable data, pre-defined discrete information]

Referring to [12] the function group name assigns a considered asset. For each function group the possible communication partners are specified to address the likelihood and to identify possible attack paths.

A more detailed description of communication requires the communication direction and the type of communication. Valid values for the communication direction are bidirectional or unidirectional. The communication type distinguishes between variable data or pre-defined discrete information. As a result the communication direction and type of communication allows determining the likelihood of an attack of a function group. In spite of this simplicity the SCPs allow to achieve the defined SecEP objective at aircraft level, i.e. to differentiate between security and non-security relevant function groups.

Analogously, parameter types and values representing the multi-system level are given in Table 2. Due to a higher level of detail during the multi-system development phase, these parameter types and values are more specific.

Table 2. Security context parameters (SCPs) on multi-system development level

Parameter Type	Valid Values
Function Name	[multi-system function name]
Communication Partner	[stakeholder, multi-system function]
Communication Interface	[ethernet, AFDX, ARINC 429, serial, discrete]
Communication Direction	[send, receive]
Type of Information for each Direction	[control data, information data]
Purpose of Use for Received Information	[forwarding, using, processing, executing]

Description of values:

Control data is data**,** which sent or received for remote control of a function by another function, e.g. turn on/off the whole entertainment function by the cabin crew management function.
Information data is data, which can be stored or displayed, but is not used for any kind of system or function control, e.g. a function which is monitored by another function provides such type of data to the monitoring function.

Forwarding information means piping the received information to other functions without using or processing it.
Using information means utilizing the received information without processing it, e.g. displaying video or audio information.
Processing information means converting and forwarding information to other functions, e.g. information is compressed, decompressed or checked and forwarding it.
Executing information means to use received information for the execution of connected functions, e.g. remote control of a function by another function.

Referring to [12] at multi-system level the function name assigns a more detailed asset. Consequently the communication partners are particularized stakeholders and more fine-grained functions, which now elaborate the likelihood and a possible attack path.

Furthermore the SCPs at this level address the interface type in a more specific way. The interface is the basis of every risk analysis because it defines the possibility that a system is attackable at all. Without any interface a system would not be attackable from an information security point of view. Defining the type of an interface as early as possible provides the opportunity to suspend specific threat scenarios.

An industry-specific interface could for instance prevent attacks of a standard malware like the worm Conficker [14] but would still be vulnerable to a specifically developed and complex malware like the worm Stuxnet [15]. Therefore an industry-specific interface like ARINC 429 which is used in the aircraft industry decreases the risk for a standard malware attack. This finally implies that the interface type allows a meaningful evaluation of the risk at this level.

At multi-system level the communication directions of each communication partner are divided into send and receive. The type of information which is exchanged, i.e. control data or information data, is assigned separately to each communication direction. The purpose of use for received information, which is detailed to forwarding, using, executing and processing information, allows a more explicit assessment of the likelihood. Additionally an allocation of possible attack paths is enabled. The defined SecEP objectives on multi-system level, i.e. to differentiate between security and non-security relevant functions, are finally achieved.

Having defined security context parameters at aircraft and multi-system level, the next step is an SCP definition at system level. At system level there is previous work on security management activities from other groups [16]. A way straightforward is to use these earlier results for structuring the SecEP at the system level. After synchronizing with the governing SEP and defining SecEP objectives at system level the SCPs can be elaborated and used analogously at the system level. This approach is fully compatible with previous work at a system level. However it resolves the challenge of a top-down approach which is globally applicable to aircraft functions and which enables standardized information exchange for security management issues across all development levels by the use of SCPs.

4 Summary and Conclusion

Increasing functionality and a rising complexity of aircraft systems leads to a complex aircraft communication network with various communication paths and partners. This progression in aircraft industry requires a reconsideration of the established systems engineering approach with emphasis to security engineering and management. To cope with the challenge of security management we have introduced the Three-V-Model representing three concurrent and interacting processes, i.e. the system engineering process (SEP), the safety engineering process (SafEP) and, for the first time, the security engineering process (SecEP). Compliant with existing guidelines and compatible to the established aircraft development process we execute the SecEP across all development levels and simultaneously to the SEP and SafEP. Defining process links and synchronizing processes on particular development levels enables an equal treatment of the SecEP. Information exchange in-between the processes is achieved by using security context parameters (SCPs). SCPs were introduced to realize a standardized communication of engineering departments and to guarantee a top-down approach for security management starting at aircraft level.

In practice, this approach enables filtering of security and non-security relevant functional information starting at the highest development level, i.e. the aircraft level and thus reduces workload on the subsequent development levels. This top-down approach using standardized communication via SCPs facilitates the collaboration of the engineering departments and clearly separates competences and work shares of neighboring departments. Moreover, this approach will particularly enable the parametric assignment of security relevant information using the model based requirements engineering methodology [17] which fosters a consistent tracking and tracing of changes during the overall development process and across all development levels.

References

1. EUROCAE / SAE: Certification considerations for highly-integrated or complex aircraft systems. EUROCAE ED-79 / SAE ARP-4754 (1996)
2. EUROCAE / SAE: Guidelines and methods for conducting the safety assessment process on civil airborne systems. EUROCAE ED-135 / SAE ARP-4761 (1996)
3. Benz, S.: Eine Entwicklungsmethodik für sicherheitsrelevante Elektroniksysteme im Automobil. PhD thesis, Universität Karlsruhe, Karlsruhe (2004)
4. EUROCAE / RTCA: Airworthiness security process specification. EUROCAE ED-202 / RTCA DO-326 (2010)
5. Hintze, H., Tolksdorf, A., God, R.: Cabin core system - A next generation platform for combined electrical power and data services. In: Proceedings of 3rd International Workshop on Aircraft System Technologies, AST 2011, Hamburg, 221-231 (2011)
6. Rosenberg, B.: Cabin Management Systems. Avionics Magazine, 26–30 (2010)
7. Ebert, C.: Systematisches Requirements Engineering, 3rd edn. dpunkt.verlag, Heidelberg (2010)
8. EASA / FAA: Equipment, systems, and installations. EASA Certification Standards 25.1309 / FAA Federal Aviation Regulations 25.1309
9. ARINC: Network domain characteristics and interconnection. ARINC 664P5 – Aircraft data network part 5 (2005)
10. ARINC: Commercial aircraft information security concepts of operation and process framework. ARINC Report 811 (2005)
11. Air Transport Association: Information Standards for Aviation Maintenance. ATA Spec 2200 (2010)
12. ISO/IEC: Information technology – Security techniques – Information security risk management. ISO/IEC 27005:2008 (2008)
13. Blanquart, J.-P., Bieber, P., Descargues, G., Hazane, E., Julien, M., Léonardon, L.: Similarities and dissimilarities between safety levels and security levels. In: Embedded Real Time Software and Systems, ERTS 2012 (2012), http://www.erts2012.org/site/0P2RUC89/8A-2.pdf
14. Nahorney, B.: The Downadup Codex - A comprehensive guide to the threat's mechanics. In: Symantec - Security Response (2009), http://www.whitepapersdb.com/whitepapers/download/1207
15. Falliere, N., OMurchu, L., Chien, E.: W32.Stuxnet Dossier. In: Symantec - Security Response (2011), http://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf
16. Bieber, P., Blanquart, J.-P., Descargues, G., Dulucq, M., Fourastier, Y., Hazane, E., Julien, M., Léonardon, L.: Security and Safety Assurance for Aerospace Embedded Systems. In: Embedded Real Time Software and Systems, ERTS 2012 (2012), http://www.erts2012.org/site/0P2RUC89/8A-1.pdf
17. Hintze, H., God, R.: A model-based security engineering process approach for the development of next generation cabin management systems (2013) (unpublished results)