Joint Safety and Security Analysis for Complex Systems

Sergey Bezzateev, Natalia Voloshina, Petr Sankin
Saint-Petersburg State University of Aerospace Instrumentation
Saint-Petersburg, Russia
bsv@aanet.ru, natali@vu.spb.ru, spetros@gmail.com

Abstract

The problem of joint safety and security analysis is considered. For complex systems method of fault tree analysis for safety and security is proposed. The effectiveness of new approach of joint safety and security analysis is shown on example of the European Railway Traffic Management System (ERTMS).

Index Terms: Safety vs. Security, Critical Systems, Fault Tree Analysis, Security Module, ETCS.

I. Introduction

Modern automated control systems are required to satisfy such critical properties as well safety and security. For each of these properties there is a number of standards that help developers to create safe or secure system.

The main problem for whole system is that the problems of safety and security for modern standards are solved separately. Safety analysis technique is described in Union Industry of Signaling (UNISIG) standards [1–10]. In these standards, safety and security are considered separately. Security analysis is realized according to security standards [11], [12]. The problem of information security analyzes for Safe systems was considered for example in [13] where the method of VPN was proposed as a decision. This decision could not be looked at as a universal one for any Safe system because of for example limited by computational resources of some part of complex system. Also the relationship with the safety was not considered. In [14–22] different aspects of safety vs. security problems were discussed and a local decision was offered as well. But there was no complex approach for joint Safety and Security problems. The Railway standard EN 50129 [23] only safety aspects are considered. Thus the main disadvantages of the methods are their not universal form, separate solution for safety and security aspects of critical system, difficulties for practical implementation of these decisions taking into account actual safety standards.

For quite time modern safety relevant system developers have been facing with new sources of risks for system safety – sabotage, informational cracking and other kinds of intrusions, it would seem a well specified system behavior. Mostly it is due to the needs of safety relevant applications to communicate to each other or to the outside world and to that important role which the increasing usage of off-the-shelf equipment and/or software plays with its often met open and public networks.

There are some inconsistencies during security and safety requirements implementation. For example to ensure high level of information security it is necessary to implement some

kind of secure methods or algorithms. This leads to increasing of the complexity of resulting system structure. As a result the safety level could occur less than it is required.

Despite of the fact that the hazards from safety and security points of view are well understood by community and well-known methodologies exist there is still no common approach developed to manage both safety and security aspects in system development. It concerns risk analysis methods, identification and alignment of integrity/assurance levels and quantification/qualification methods of possible errors.

A safety analysis usually starts with identification of the core hazard and then examining potential failure modes that could cause that hazard but a security analysis considers a rather different set of potential threats and undesirable consequences.

It is highly important to create an approach for safety vs. security analysis using modern standards that could be easily integrated into safety or security standards.

The most important task is to find the way how to take into account security problems while safety analysis. For complex and critical systems it is necessary to provide a high level of safety that means that the probability of system failure should be less than required value depending on the type of the complex critical system. Safety level is checking while system design according to the corresponding safety standards and should be guaranteed for resulting Safe System. But for modern complex systems especially automated ones the problem of information security become more critical. The usage of telecommunication technologies in control subsystem of complex system increases its efficiency but also leads to information security problems. To provide information security special methods and algorithms should be implemented according to information security standards [11], [12]. Thus additional information security modules should be realized and integrated into Safe System. This integration could cause new hazards and greatly reduce resulting Safety level of whole Complex System. As a result the hazards of potential failures to be avoided should be detected. These hazards should be both for safety and security aspects.

This paper is devoted to find the method to solve the safety vs. security problem for such critical systems taking into account a current safety and security standards. The European Railway Traffic Management System (ERTMS) is taken as an example of Complex System.

II. Security analysis for safety standards

To provide the high level of Safety for automated system it is necessary to implement special information security methods and algorithms realization of which can be looked at as a single Safety Module of the whole system. This way it is possible to imbed an analysis of information security problems influence into standard Safety analyzes and to estimate resulting Safety level.

With this approach Security hazards become a Hazards of Security Module. This idea is represented graphically on Fig. 1. These hazards of such Security Module could be analyzed according to the common safety analysis technique for example fault tree analyzes (FTA) [6].

The feather safety analyzes with security aspects according to proposed Safety Module approach will be shown on example of the Eurobalise subsystem of ETCS.

A. Security module for representation of the hazardous events

Eurobalise Transmission System is the Pan-European spot transmission system for transmission between wayside and the ERTMS/ETCS Kernel. It is a sub function in the

total European Rail Traffic Management System, ERTMS, and it is one of the sub-systems in the railways European Train Control System, ETCS.

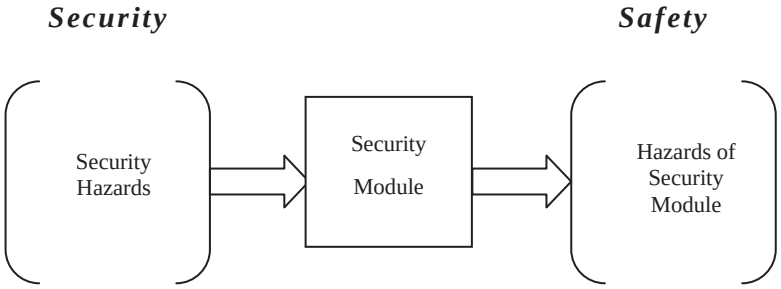

Fig. 1. The Basic Principle of the Security Module

The Eurobalise (also called Balise) is a single device mounted on the track between the rails of a railway, which communicates with a train passing over it. It is spot transmission equipment which is based on a passive RFID transponder.

Balise Transmission Module (BTM) is an On-board module for intermittent transmission between track and train that processes Up-link as well as Down-link signals and telegrams from/to a Balise. It interfaces the ERTMS/ETCS Kernel and the Antenna Unit. Data transmitted from track to train is considered as safety critical telecommunication [1].

Graphical representation of the main blocks of ETCS and its hazardous events within the UNISIG Reference [7] is shown on the Fig. 2. The hazardous events named by the names of corresponding blocks and arrows show the path of influents on kernel element. For Eurobalise subsystem there are BTM – H hazards from Balise Transmission Module side and EUB-H from Eurobalise side. Their description is given in the part 3 of the UNISIG subset 088 [6]. Initially there were no hazardous events associated with information security problems. To take into account these problems the proposed Security Module was integrated into this scheme and corresponding hazardous events were named SMB-H.

B. Security hazard analysis for Eurobalise of ETCS

After adding the Security Module the Security Module Hazards could be considered. It's important to notice that Security Module Hazards could be caused by Security and Safety problems both. Safety hazards of Security Module mean that this module could work in a wrong way. Security hazards of Security Module mean that this module could be broken by the attacker. This separation of Security Module Hazards is shown on Fig. 3.

C. Fault tree analysis with Security module

One of the standard methods for Safety analyzes is a Fault Tree Analyzes (FTA) [6].

Fault trees for Security Module could be constructed similar to the other ordinary fault trees in the Eurobalise subsystem.

The identified system level transmission hazards that apportioning between the onboard and trackside are defined by the standard as:

- TRANS-BALISE-1 - Incorrect balise group message that is received by the onboard kernel functions as consistent - (Corruption).

- TRANS-BALISE-2 – Balise group not detected by the on-board kernel functions – (Deletion).

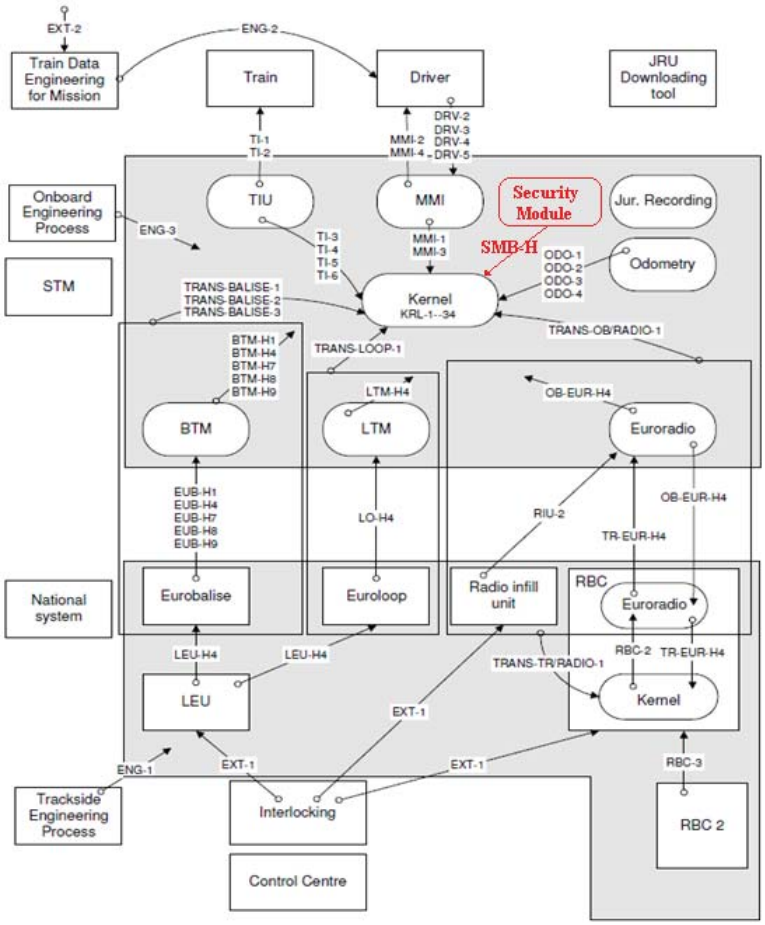

Fig. 2. Graphical representation of the hazardous events with Security Module

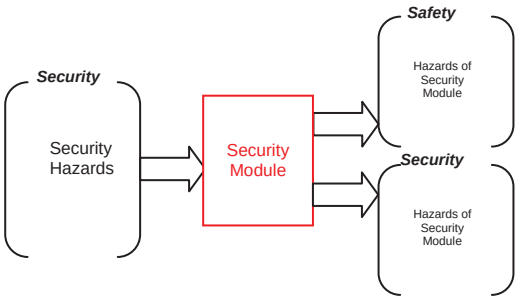

Fig. 3. Security Module Hazards separation

- TRANS-BALISE-3 – Inserted balise group message received by the on-board kernel functions as consistent – (Cross Talk).

These three hazards have been identified as part of the Failure Modes and Effects Analysis (FMEA) on the transmission systems. These hazards are the base events of the functional fault tree in part 1 of Subset 088[6].

Thus the list of Security Module Hazards created according to Safety standards was defined as:

- SMB-H1 – A balise group is not detected, due to the failure of security module.
- SMB-H4 – Transmission of an erroneous telegram interpretable as correct, due to failure of security module.
- SMB-H7 – Erroneous localization of a Balise Group, with reception of valid telegrams, due to failure of security module.
- SMB-H8 – The order of reported Balises, with reception of valid telegram, is erroneous due to failure of security module.
- SMB-H9 – Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failure of security module.

It is important to notes that these hazards are the results of the standard failures, but they are caused by Security Module. New Fault trees with added security module hazards SMB-H for TRANS-BALISE-1, TRANS-BALISE-2 and TRANS-BALISE-3 are shown on Fig. 4–6.

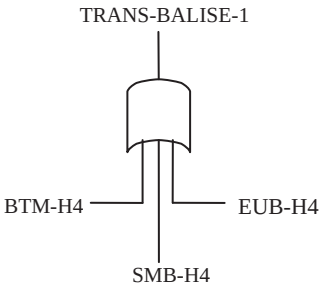

Fig. 4. Fault tree for TRAN-BALISE-1 (corruption)

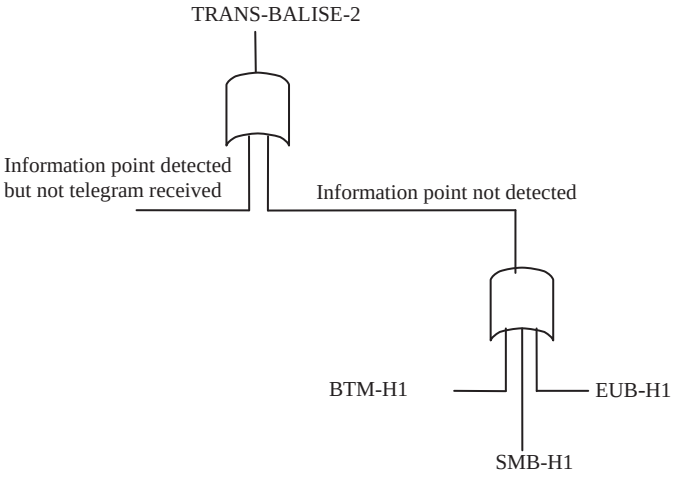

Fig. 5. Fault tree for TRANS-BALISE-2 (deletion)

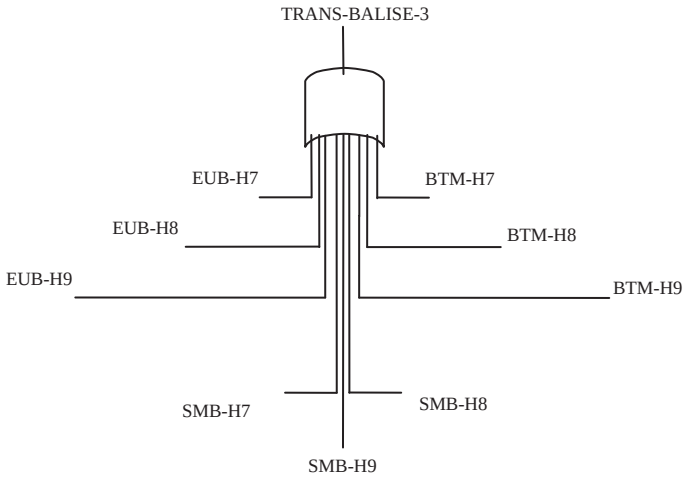

Fig. 6. Fault tree for TRANS-BALISE-3 (Insertion or Cross Talk)

The Security Hazards from attacker has been converted to hazards of Security Module. To estimate the resulting safety level of the System the probability of these Security Module Hazards could be calculated. The value of this probability depends on the architecture of Security Module, conditions of its work and realization.

D. Example of Fault Tree Analysis of Security Module for Eurobalise

In modern ETCS safety standard there is no information security hazard analyzes and information security modules does not described for Eurobalise subsystem. But Eurobalise module is based on RFID (radio frequency identification) telecommunication technology. According the information security standard [11] it is necessary to organize information protection for data transmitted by Eurobalise subsystem.

From information security standards such Security problems could be formulated as:

- Integrity problem
- Availability problem
- Confidentiality problem

These information security problems could appear because of different kind of attacks such as masquerade, blocking and message corruption, etc.

For ETCS Eurobalise subsystem one of the most critical attacks is a masquerade that can cause an integrity problem of ERTMS. For example, for current standards of ETCS it's easy to make a copy of any balise, change another balise by this copy. This change may cause a core hazard of ETCS. This situation could dramatically reduce the resulting Safety level of ERTMS. To avoid such attack it is use to apply one of authentication algorithms. The main requirements for authentication module are that the protocol could be realized on passive RFID elements and authentication module could be easily integrated in ERTMS system Eurobalise subsystem.

In this research we consider to analyze the authentication module in Eurobalise subsystem that realizes LMAP++ authentication protocol [24] as an example of Security Module. According to our approach the scheme of Security Module of Authentication (SMA) is shown on Fig. 7.

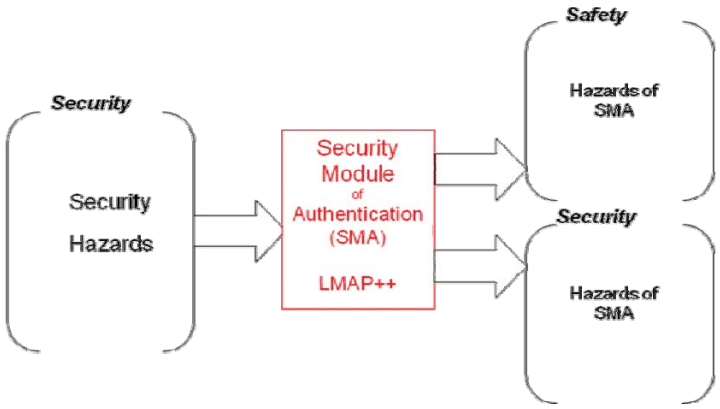

Fig. 7. Security Module Hazards scheme for authentication module

After Security and Safety analysis the following hazards list for authentication module was defined. This list consists of the safety and the security hazards of Security Module (authentication LMAP++ module). These hazards (SMAB-H) and corresponding origins of failure are represented in TABLE I.

TABLE I
HAZARDS LIST FOR AUTHENTICATION MODULE

Tipe of Security Module Hazard	No.	Hazard Description	Origin of failure
Safety hazards of Security Module	SMAB-H1	The Balise is not detected	Security module
	SMAB-H2	Wrong authentication	Security module
	SMAB-H3	Delay	Security module
Security hazards of Security Module	SMAB-H4	Successful Brute force Attack	Attacker
	SMAB-H5	Successful Desynchronization Attack	Attacker

New hazards could be added to existing Fault tree analysis (FTA). The standard TRANS-BALISE hazardous events such as Corruption, Deletion and Insertion could be analyzed considering the problems of masquerade attack. For this example it is possible to estimate probability of security hazards of security module of authentication. Safety hazards could be calculated by standard Safety analysis technique.

Here is an example of security hazards of authentication module based on authentication protocol LMAP++ [24] calculation. The choreography of LMAP++ protocol is shown on. Fig. 8 .

Procedure of keys updating in LMAP++:

$K1new = (K1 \oplus n)+(IDS + K2 + ID)$,

$K2new = (K2 \oplus n) + (IDS + K1 + ID)$,

$IDSnew= ((IDS + K1) \oplus n)+((ID+ K2) \oplus n)$.

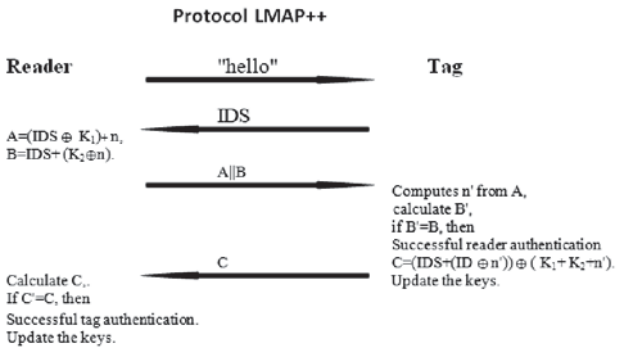

Fig. 8. Choreography of LMAP++

Where:

- IDS — dynamic identifier of tag, change after every successful authentication,
- ID — static identifier of tag, stored in the safe area of memory,
- n — random number which is produced by RFID reader,
- K1, K2 — secret keys changes after every successful authentication. They are stored in the safe area of memory of RFID tag and reader,
- A;B;C — messages, which are transmitted during the authentication process,
- “hello” — message/command, which initializes the beginning of authentication protocol.

By using such mutual authentication protocol and therefore by adding to ETCS system additional security module we solve the problem of fault probability generalized by security problems that can be estimated as equal to 1 without information protection. Certainly it is impossible to achieve this probability equal to 0 but it is possible to get significant reduction of its value. By adding security module we obtain the improvement in security but we naturally have new probability of the safety for such new block and as a result a new Safety level for whole System. This probability can be calculated by the ordinary methods and depends on implementation features of this additional security module. Fault probability by security problems for security module in our new scheme (with additional security module for mutual authentication) depends on possible attacks on protocol provided by security module (in our example it is LMAP++). As an example we would consider only one such attack here – desynchronization.

Desynchronization attack on LMAP++ proposed in [24] is bases on properties of the identity of addition modulo 2^m and XOR operations for the least significant bit (LSB) and the probability equal 2^{-4}, that LSB of IDS, ID, K1, K2 equal to zero, i.e. $IDS_0=ID_0=[K1]_0=[K2]_0=0$.

For one balise an attacker can have success in desynchronization attack with probability 2^{-4}.

In ETCS the groups of balises are used. Number l of balises in one group is from l=3 to l= 8. For example the failure analyze of motion direction determination risk should be performed. The fault probability by security problems of this type for security module (psm) could be estimated as $psm=(2^{-4})^{l-1}$, $2^{-28} \leq psm \leq 2^{-8}$.

The influence of subjected Security Module is shown on Fig.9-11.

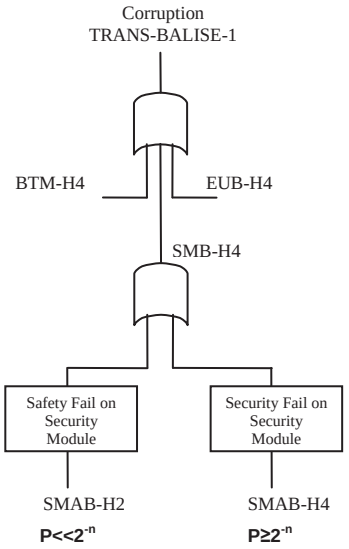

Fig. 9. FTA for TRANS-BALISE-1 with SMAB, where n- length of secret key

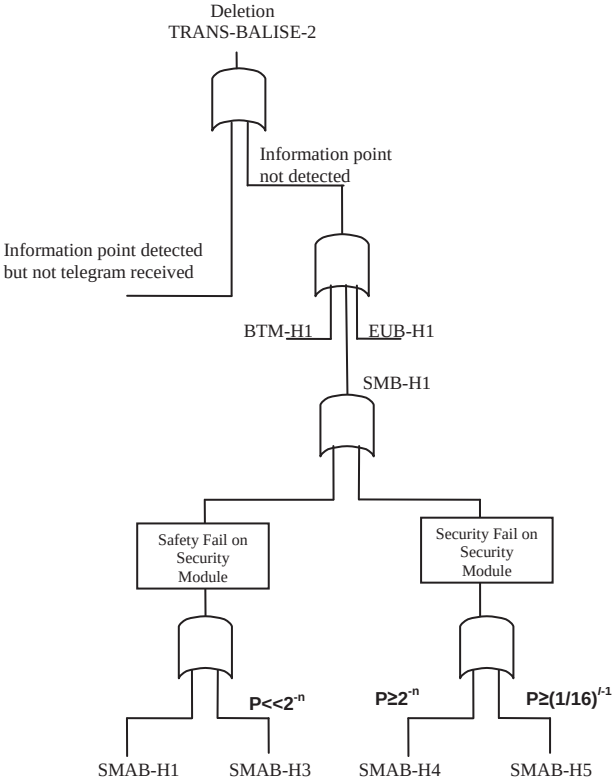

Fig. 10. FTA for TRANS-BALISE-2 with SMAB, where n- length of secret key, *l*- number of balises in a group

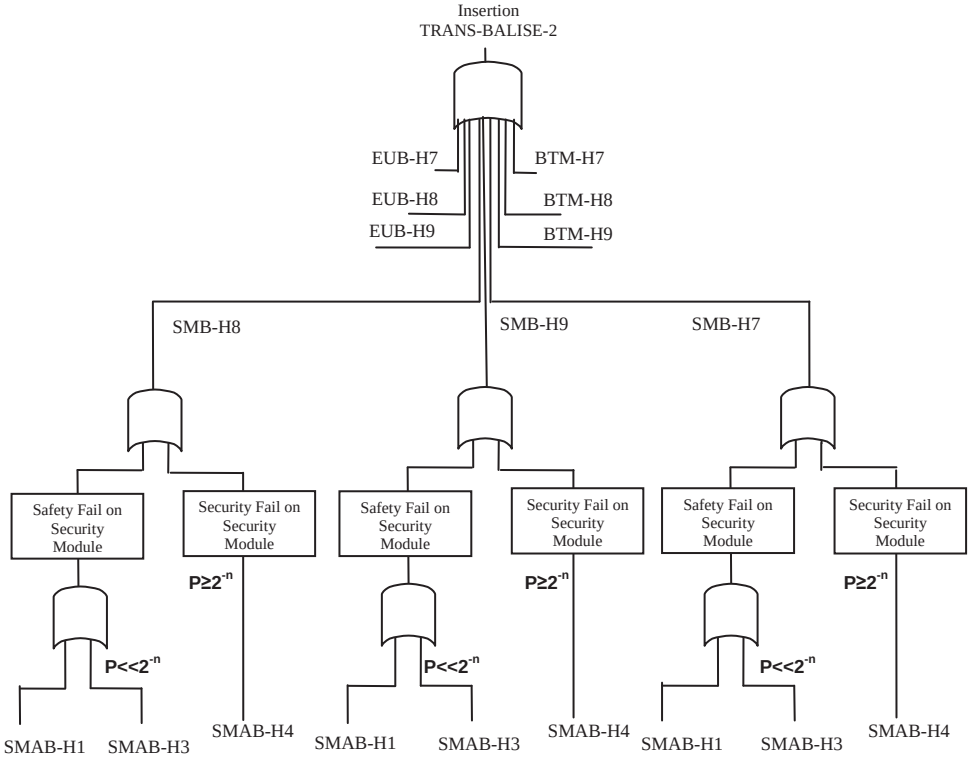

Fig. 11. FTA for TRANS-BALISE-3 with SMAB, where n- length of secret key

This Figures show that Security Module influences at every part of Eurobalise subsystem. The total resulting Safety level of the System becomes higher because the probability of security hazards becomes much less than 1.

As a unification of this concept the Security system could be represented as a Security Module of ETCS. It should interact with other parts of ETCS which could be associated with security problems.

To get real Safety level of Automated System it is necessary to analyze Security Module for whole System that can be rather complex task.

III. Conclusion

The problem of Safety vs. Security for critical systems was analyzed. It was found that there is no concerted method to develop safe and secure systems by using actual safety and security standards. The safety standards for ETCS were analyzed. It was found that for ETCS there is no consideration of security hazards. It was suggested to add a special Security Module to take into account a Security Hazards for standard fault tree analyses of safety. The Security Hazards for Eurobalise part of ETCS were defined corresponding to Subset 036. The Safety-Security Fault tree example was built. As an example of realization of the proposed method the safety analysis of the Eurobalise of ETCS was considered. Results of numerical calculations of safety with security for the selected Eurobalise block of ETCS were proposed. It was shown that total level of System Safety could be increased by using Security Module.

REFERENCES

[1] FFFIS for Eurobalise, ERTMS/ETCS – Class 1, Subset 036, UNISIG, 2007.
[2] Euroradio FIS, ERTMS/ETCS – Class 1, Subset 037, UNISIG, 2005.
[3] Off-line Key Management FIS, ERTMS/ETCS – Class 1, Subset 038, UNISIG, 2008.
[4] Unisig Causal Analysis Process, ERTMS/ETCS – Class 1, Subset 077, UNISIG, 2003.
[5] Failure Modes and Effects Analysis for the Interface to/from an Adjacent RBC - in Application Level 2, ERTMS/ETCS – Class 1, Subset 078, UNISIG, 2007.
[6] Safety Analysis, ERTMS/ETCS – Class 1, Subset 088, UNISIG, 2008.
[7] Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, ERTMS/ETCS – Class 1, Subset 091, UNISIG, 2009.
[8] ERTMS EuroRadio. Conformance Requirements, ERTMS/ETCS – Class 1, Subset 092-1, UNISIG, 2006.
[9] ERTMS EuroRadio. Test cases. Safety Layer, ERTMS/ETCS – Class 1, Subset 092-2, UNISIG, 2006.
[10] System Requirements Specification. ERTMS/ETCS – Baseline 3, Subset 026, UNISIG, 2008.
[11] IEC 15408 – Information technology – Security technique – Evaluation criteria for IT security, 2005.
[12] IEC 17799 – Information technology – Security techniques – Code of practice for information security management, 2005.
[13] Kristoffer Hedberg, Fredrik Elestedt, *Safety-critical Communication Controllers for Railway Signalling in Public Networks*. Chalmers University of Technology, Gothenburg, 2008.
[14] Dr Robert Stroud and Professor Robin Bloomfield, From Safety to Security – how secure is ERTMS?, IRSE NEWS, Issue 176, March 2012.
[15] ETCS Implementation Handbook, UIC, 2008.
[16] Railway Group Standard, GC/RT5201, Lineside Security, 1999.
[17] Esposito Rosaria, Lazzaro Armando, Marmo Pietro, Sanseviero Angela, Formal Verification Of Ertms Euroradio Safety Critical Protocol. *In Proceedings 4th Symposium on Formal Methods for Railway Operation and Control Systems (FORMS'03)*, Budapest. L'Harmattan Hongrie, 2003.
[18] Functional Safety Analysis of ETCS DMI. *Final Safety Analysis Report for European Railway Agency*, 2009.
[19] Thomas Novak, Albert Treytl, Peter Palensky. Common Approach to Functional Safety and System Security in Building Automation and Control Systems. Emerging Technologies and Factory Automation, *ETFA*, 2007.
[20] U.S. Department of Transportation Federal Transit Administration. Safety and Security Management in Rail Transit Projects, FTA Office Of Safety And Security, 2009.
[21] Saad Zafar and R. G. Dromey, Integrating Safety and Security Requirements into Design of an Embedded System. *Software Engineering Conference, APSEC '05*. 12th Asia-Pacific, 2005.
[22] J. Smith, S. Russell, M. Looi, Security as a Safety Issue in Rail Communications. *Conference: Australian Workshop on Safety Critical Systems and Software - SCS*, 2003, pp. 79-88.
[23] EN 50129. Railway Applications - Communication, Signalling And Processing Systems - Safety Related Electronic Systems For Signalling. CENELEC, 2003.
[24] Masoumeh Safkhani, Nasour Bagheri, Majid Naderi, Somitra Kumar Sanadhya, "Security Analysis of LMAP++, an RFID Authentication Protocol", *6th International Conference on Internet Technology and Secured Transactions*, 11-14 December 2011, pp. 689-694.