Joint Safety and Security Analysis for Complex Systems

Sergey Bezzateev,
Natalia Voloshina,
Petr Sankin

Safety vs. Security

Information security

is a Hot point

of any Critical System

ERTMS

One of the most critical systems is

European **R**ail **T**raffic **M**anagement **S**ystem (**ERTMS**)

Is an EU “major European industrial project” to enhance cross-border interoperability and signalling procurement by creating a single Europe-wide standard for railway signalling with the final aim of improving the competitiveness of the rail sector.

Safety vs. Security for ERTMS

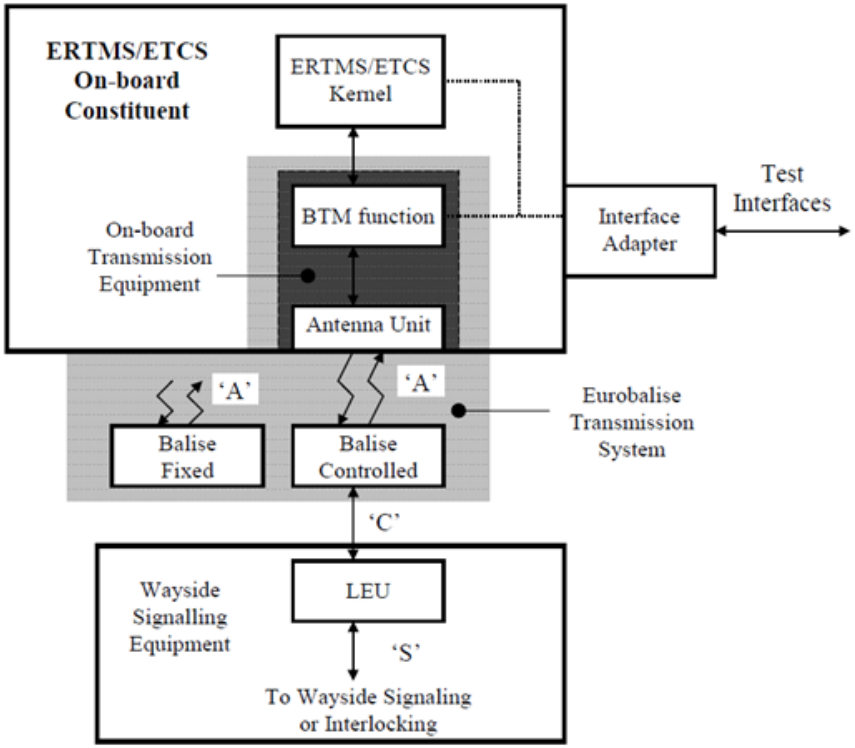
It is critical to ensure the high level of

ERTMS Safety

Safety level depends on

Information Security

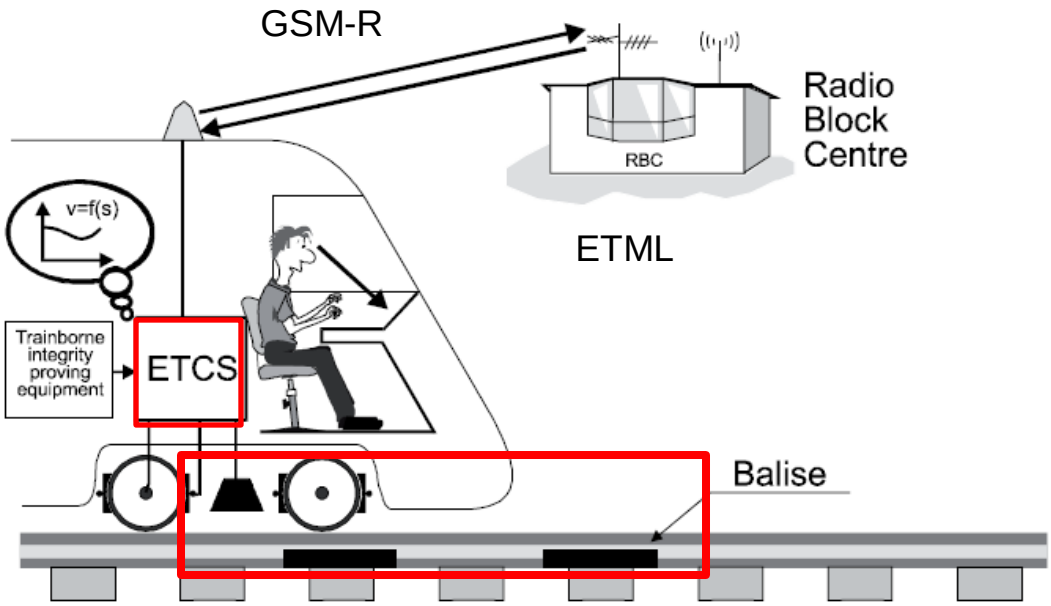
Eurobalise Transmission System



Eurobalise

1. *stores* infrastructure data as pre-formatted 'telegrams' :
   - •position reference,
   - •speed limits,
   - •line gradient,
   - •works on the line,
   - •etc.
2. *sends* to train movement authorities and trackside data (telegrams selected by LEU) when energised by power from train's antenna.

How to balise work?



Hazards for Eurobalise

Safety Analysis defines hazardous events for balise system in ETRC:

HAZARDOUS EVENTS
TRANSBALISE-1(Corruption)
Incorrect balise group message received by the on-board kernel functions as consistent
TRANSBALISE-2(Deletion)
Balise group not detected by on-board kernel functions (deletion)
TRANSBALISE-3(Insertion)
Inserted balise group message received the on-board kernel functions as consistent

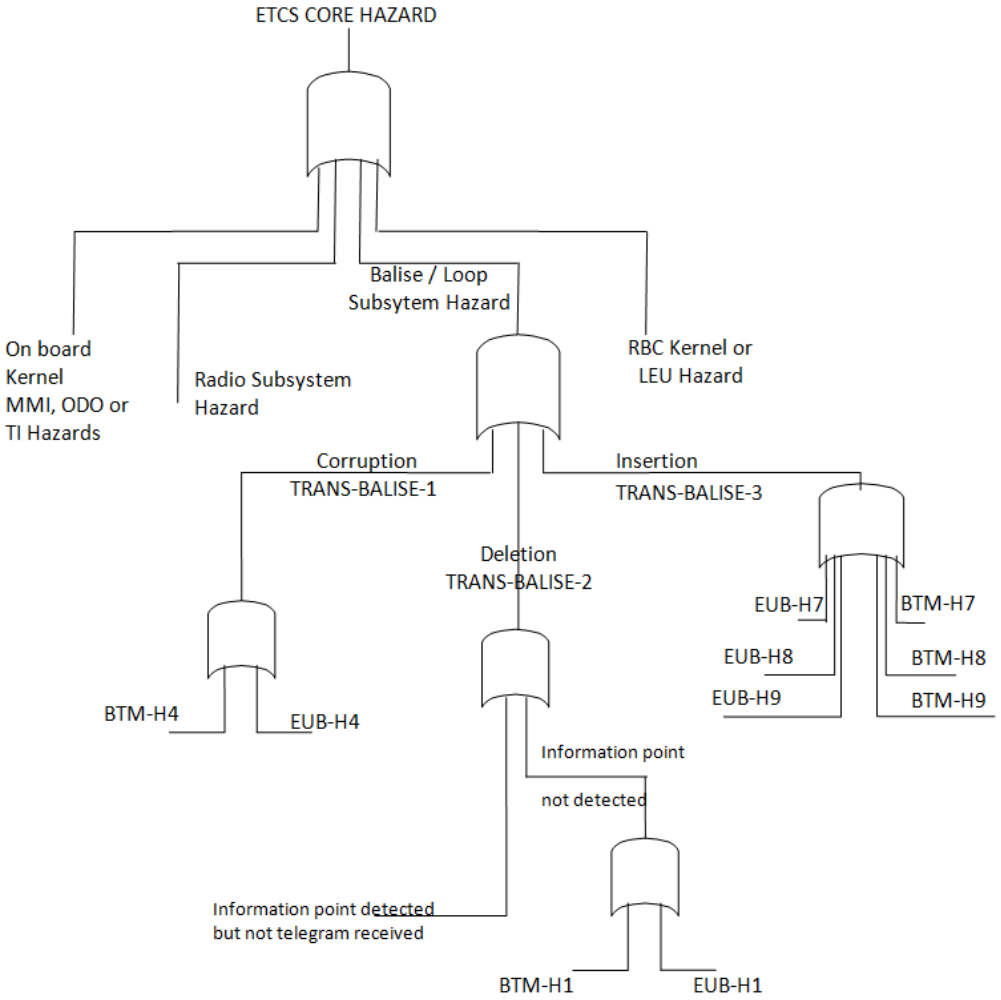
Hazardous Events for Balise System in ETRC

The subordinate hazards to TRANS-BALISES are defined as:

EUB-H1 A balise group is not detected, due to failure of a balise group to transmit a detectable signal
EUB-H4 Transmission of an erroneous telegram interpretable as correct, due to failure within a Balise
EUB-H7 Erroneous localisation of a Balise Group, with reception of valid telegrams, due to failure within Balises (too strong up-link signal)
EUB-H8 The order of reported Balises, with reception of valid telegram, is erroneous due to failure within a Balise (too strong up-link signal)
EUB-H9 Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failures within Balises (too strong up-link signal)

BTM-H1 A balise group is not detected, due to failure within the onboard BTM(Balise Transmission Module) function
BTM-H4 Transmission to the on-board kernel of an erroneous telegram, interpretable as correct, due to failure within the onboard BTM function
BTM-H7 Erroneous localisation of a Balise Group, with reception of valid telegrams, due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal)
BTM-H8 The order of reported Balises, with reception of valid telegrams, is erroneous due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal
BTM-H9 Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal)

Fault Tree Analysis



Security problems of Safety Analysis

Currently

Safety Analysis

and

Information Security Analysis

are made

separately

The goal of the research

To find the method

how to take into account

the Information Security problems

while Safety Analysis

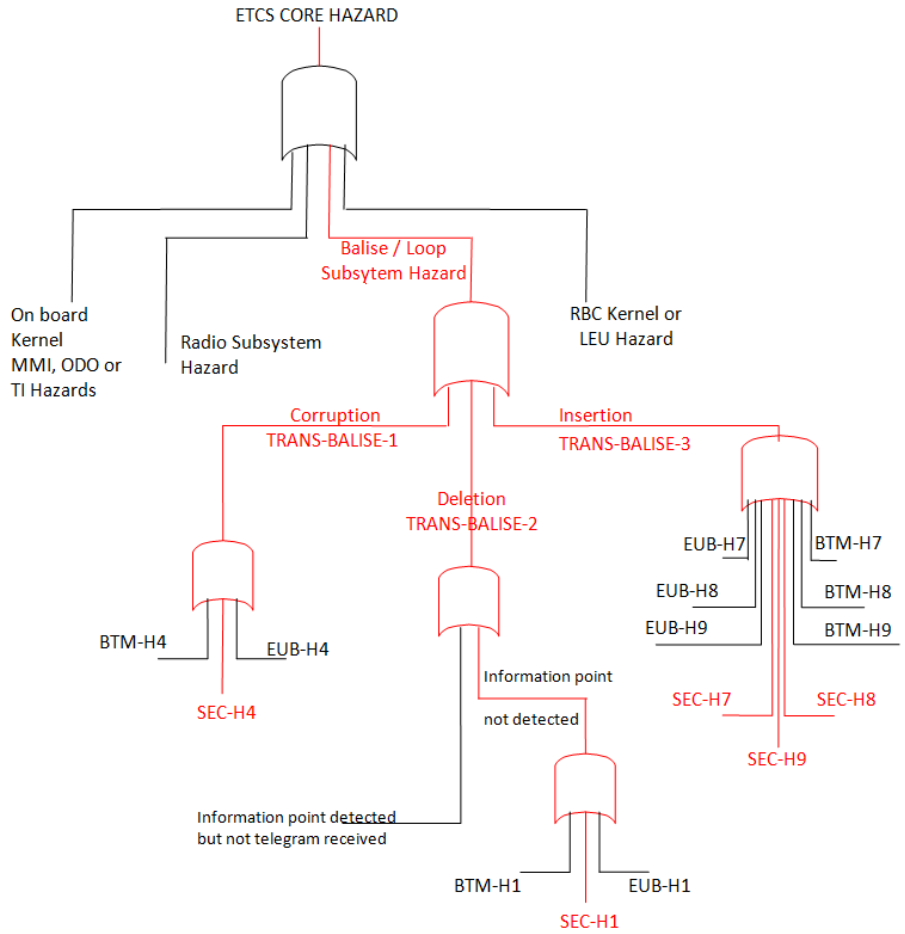
based on

existing Safety and Security standards

Security Hazards List

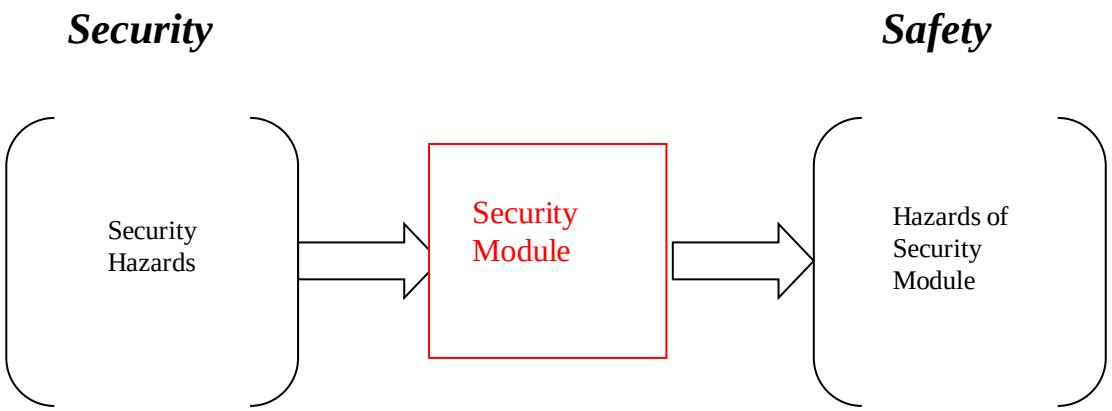
- SEC-H1 – A Balise is not detected due to the attacker.
- SEC-H4 – Transmission of an erroneous telegram interpretable as correct due to the attacker.
- SEC-H7 - Erroneous localisation of a Balise with reception of valid telegram due to the attacker.
- SEC-H8 – The order of reported Balises, with reception of valid telegram, is erroneous due to the attacker.
- SEC-H9 – Erroneous reporting of a Balise in a different track, with reception of valid telegram due to the attacker.

Fault Tree with Security Hazards

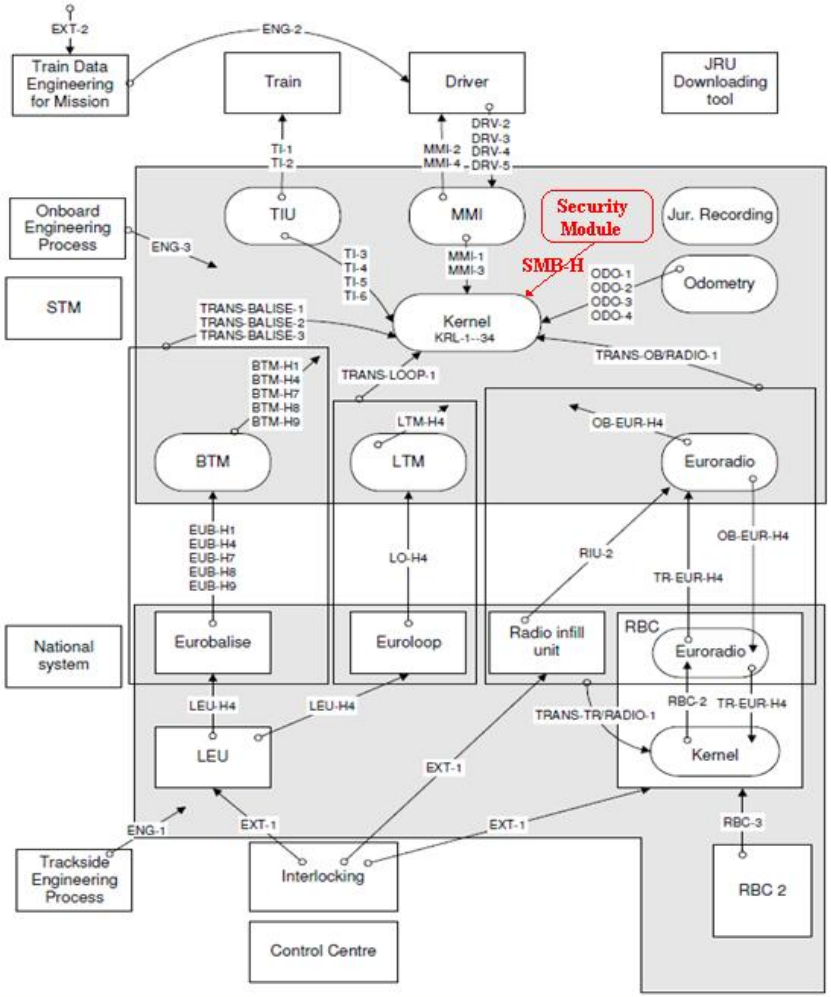


Without implementation of special information security methods the probability of successful attack is equal to 1!

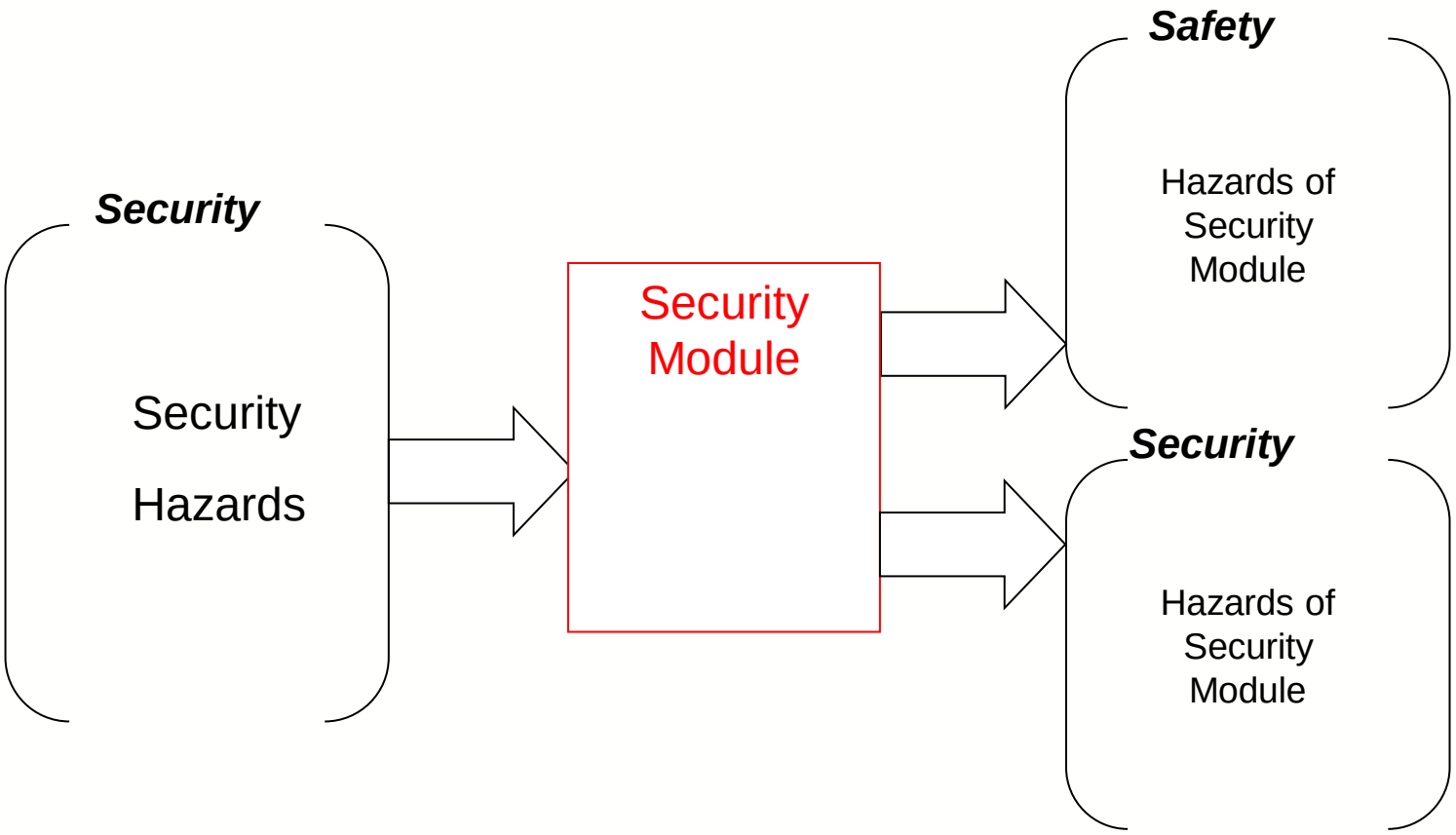
Security Module Approach



Graphical representation of the hazardous events of ETCS



Security Module

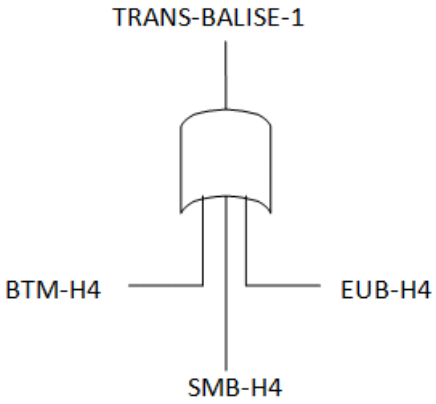


The List of Security Module Hazards:

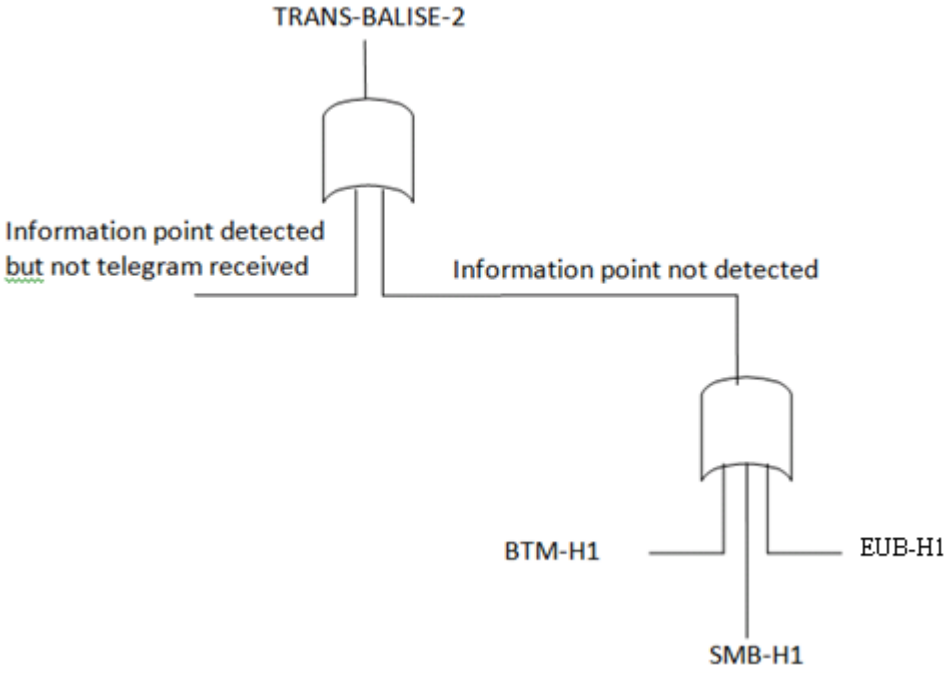
- **SMB-H1** – A balise group is not detected, due to the failure of security module.
- **SMB-H4** – Transmission of an erroneous telegram interpretable as correct, due to failure of security module.
- **SMB-H7 -**– Erroneous localization of a Balise Group, with reception of valid telegrams, due to failure 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.

Fault Trees with Security Module

Corruption

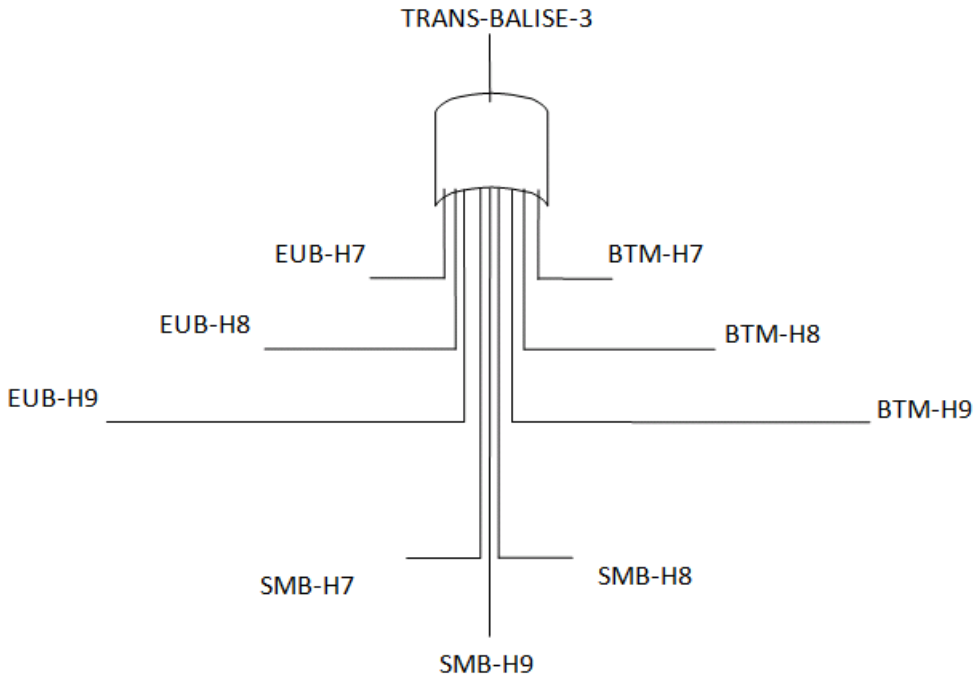


Deletion

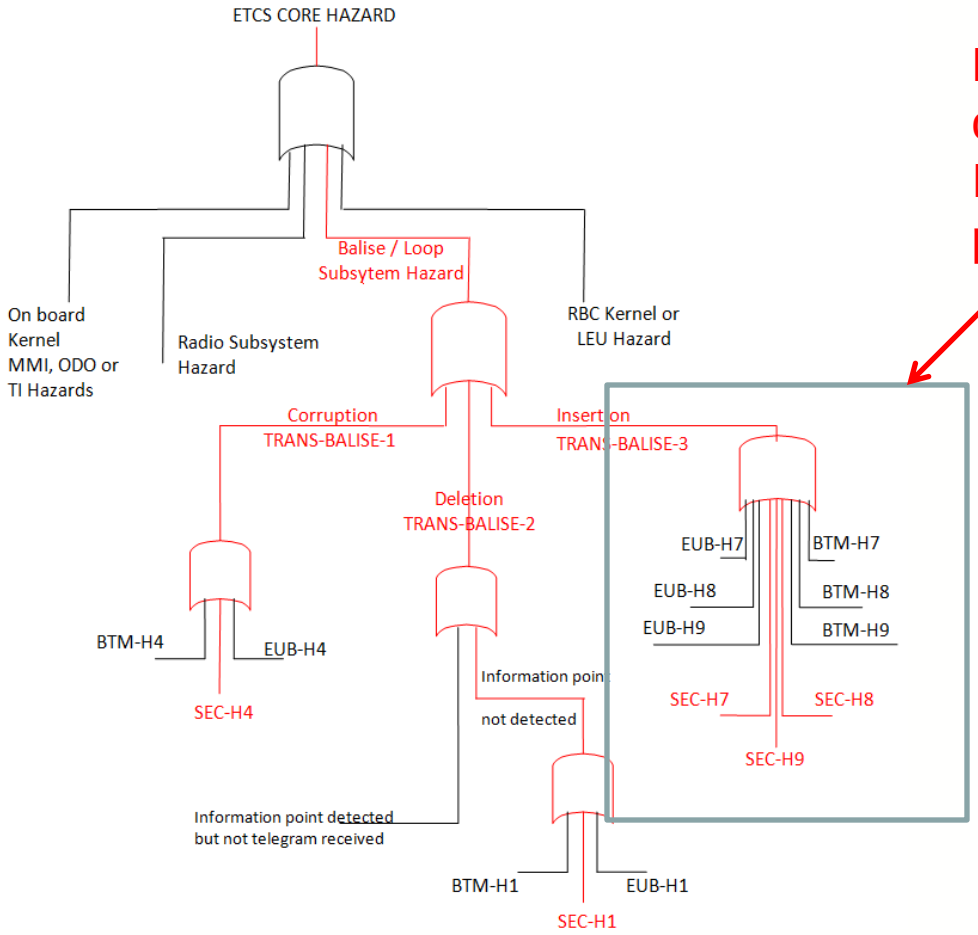


Fault Tree for Insertion/Cross Talk

Insertion

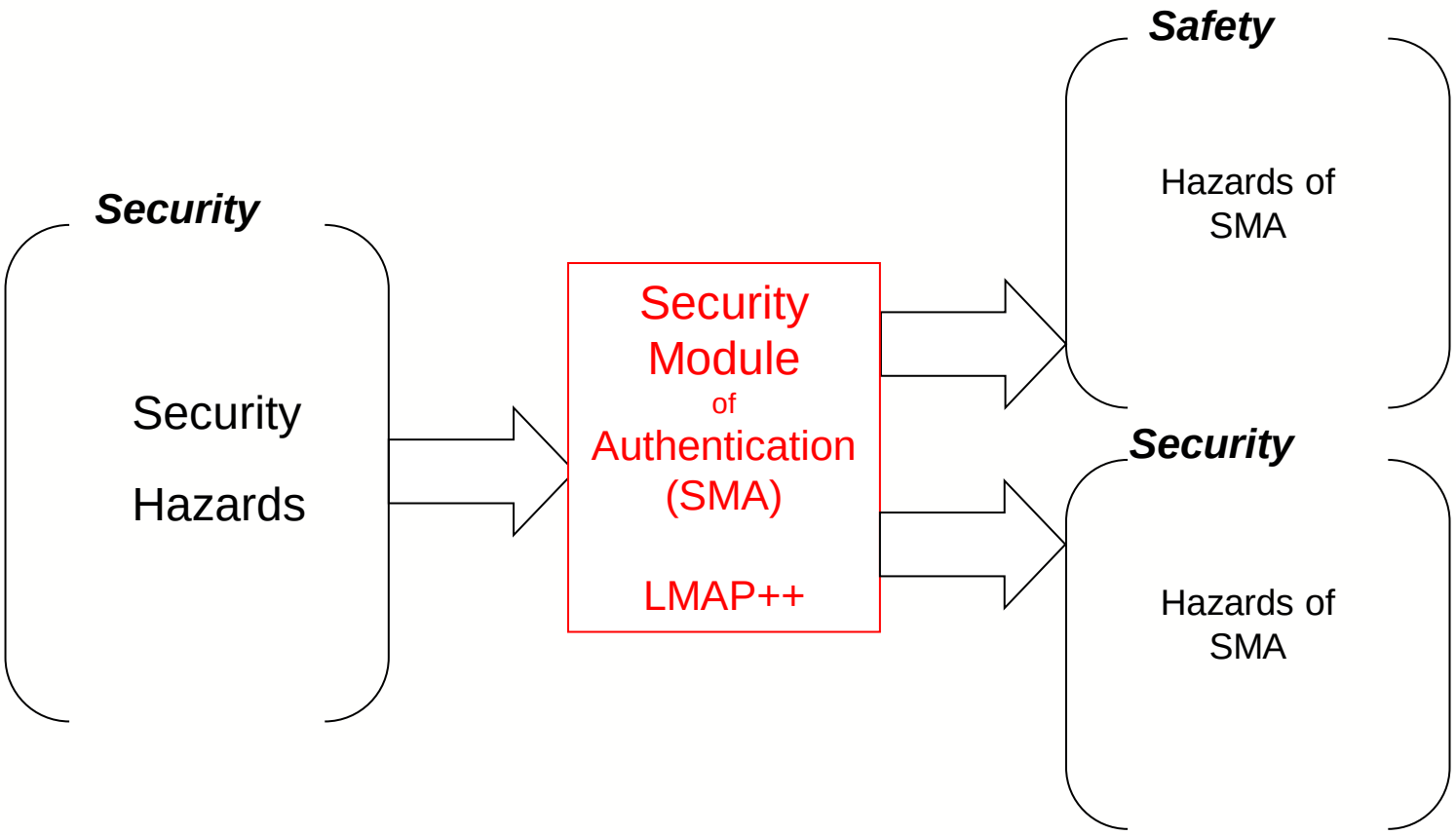


Example attack on Eurobalise



Masquerade attack on Eurobalise –> Integrity security problem

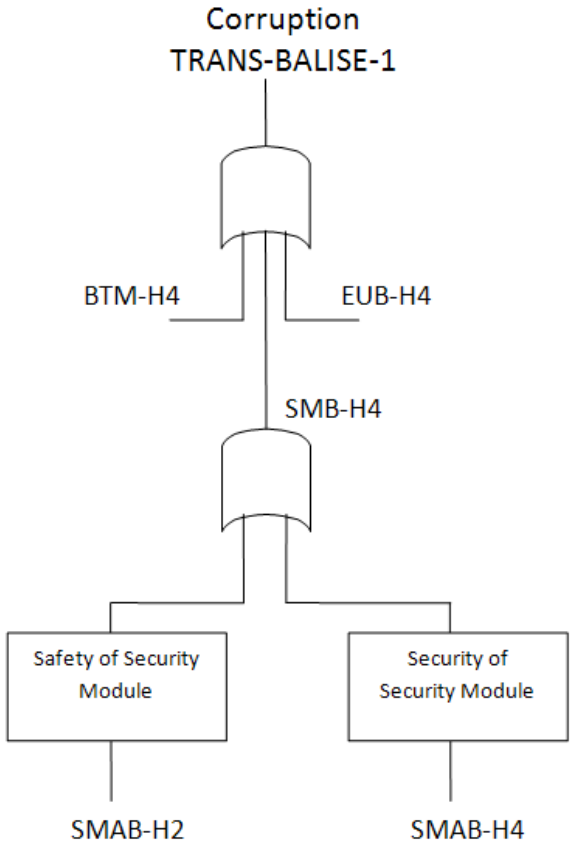
Security Module



Hazards List for Authentication Module

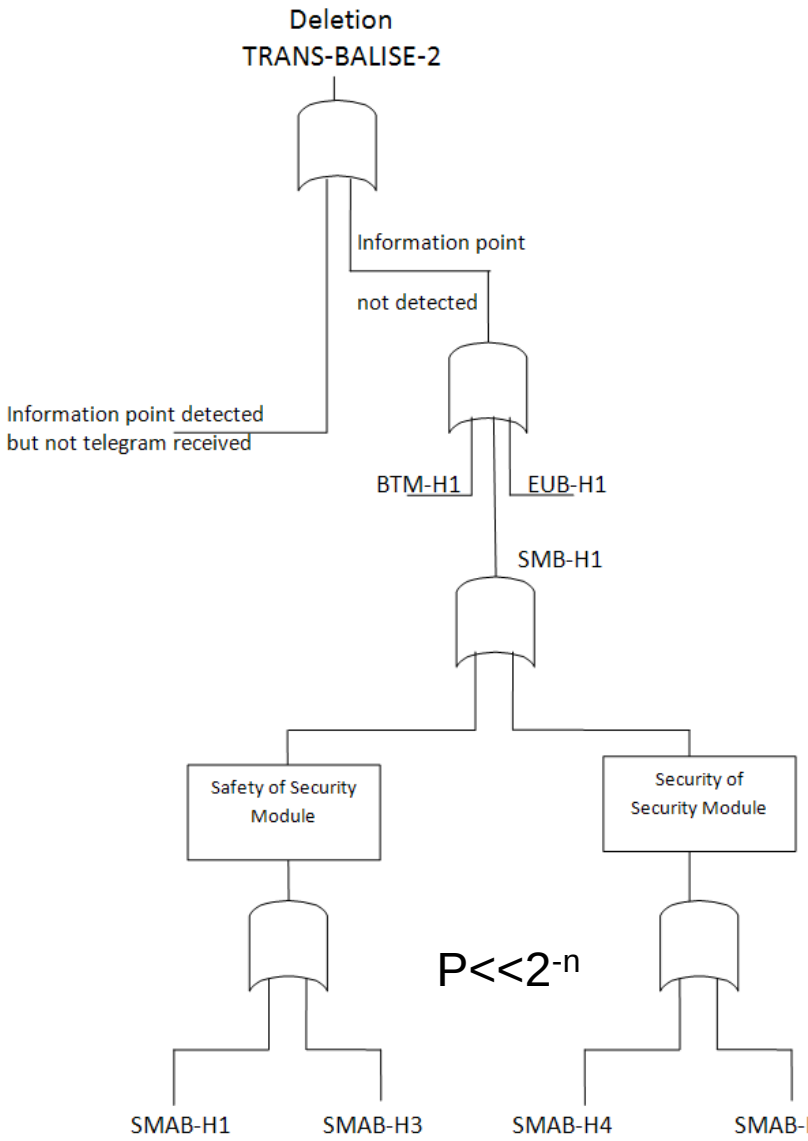
Type of Security Module Hazard	No.	Hazard Description	Origin of failure
Safety hazards of Security Module	SMAB-H1	The Balise is not detected	Security module
	SMAB-H2	Wrong authentication	Security module
	SMAB-H3	Delay	Security module
Security hazards of Security Module	SMAB-H4	Successful Brute force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

FTA for TRANS-BALISE-1 with SMAB



$P<<2^{-n}$ $P>=2^{-n}$

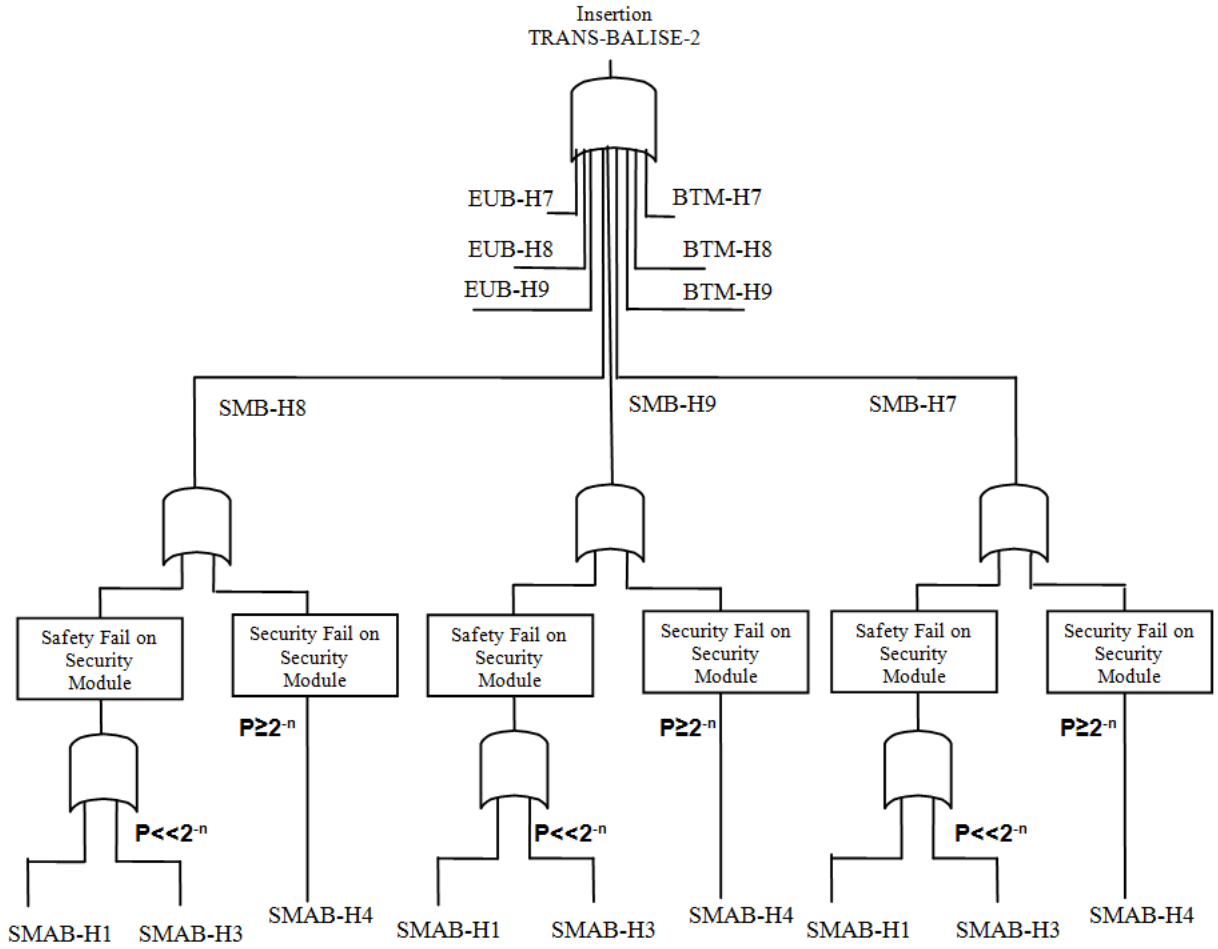
FTA for TRANS-BALISE-2 with SMAB



$P << 2^{-n}$

$P >= (1/16)^{m-1}$

FTA for TRANS-BALISE-3 with SMAB



Conclusion

- 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.
- It was shown that total level of System Safety can be increased by using Security Module.

Q&A

Thank your for attention!