Operational Security – A Coming Evolution of Railway Operational Procedures Under the IT Security Threat

Po-Chi Huang(✉) and Birgit Milius

Institute of Railway Systems Engineering and Traffic Safety (IfEV),
Technische Universität Braunschweig, Braunschweig, Germany
{po-chi.huang,b.milius}@tu-braunschweig.de

Abstract. The railway system has benefited from the rapid technology revolution since the 1990s. The mechanical and manpower intensive railway system has gradually evolved into a centralize- and digital-controlled, information- and communication-based system. IT security was not considered during the system (re)design. This paper begins with discussing the need and absence of procedures to sustain operations when an IT security breach has occurred or is suspected.

Then operational security is introduced. It is a new research field which focuses on operational procedures taking into account the effects of safety as well as security-related changes in the system e.g. due to failures or threats. The scope of operational security and general requirements on operational procedures will then be discussed. Lastly, we give an outline of a proposed project with its planned work packages.

Keywords: Operational security · Functional safety · IT security · Railway operation · Degraded operation · Operational procedures · Railway safety

1 IT Security – Evolutional Challenge to Railway Operation

The railway system has hugely benefited from the rapid development of Information and Communication Technology (ICT or commonly IT) since the 1990s and begins its own journey of evolution. The old-fashioned mechanical and manpower intensive railway system has gradually evolved into a centrally and digitally controlled, information- and communication-based system. Today, IT is widely used in railways. The achievements of technical systems and operation modes like European Train Control System (ETCS), Automatic Train Operation (ATO) and Operation Control Center (OCC) all took place with benefits of the IT development.

The issue of IT security is not a new topic in IT industry, it accompanies the development of IT since the beginning. But for the railway sector, IT security was not considered as a serious issue in the past as the railway system conventionally used proprietary, that are hard to hack, systems. The situation changed when the economic efficiency, privatization, modernization and the liberalization of railway systems became a requirement for the railway sector. The increasing use of commercial off-the-shelf (COTS) products makes the modern railway system affordable and flexible, but also more vulnerable.

T. Lecomte et al. (Eds.): RSSRail 2016, LNCS 9707, pp. 69–78, 2016.
DOI: 10.1007/978-3-319-33951-1_5

Considering the potential vulnerabilities and threats which come with using COTS products, the issue of IT security has received further attentions in the railway sector, especially for safety related technical systems. Railways is considered as a critical infrastructure, which means that it needs to retain its operation even in abnormal situations [1]. Safety is the core value of the railway system. However, shutting the railway system down when an IT security breech is suspected might be the safe option, but is not feasible and not acceptable. To fulfill the requirement of continued safe operations when facing IT security threats, a holistic view of the operational procedures taking into account safety- and security issues is necessary.

2 Operational Continuity – A Deficiency in Work of IT Security

As mentioned previously, the issue of IT security has received some attention in the railway sector during the last few years. Not only researchers, but also public authorities and standard committees have realized the possible severity of IT security threats on the railway system and the urgent need of countermeasures. For example, with the funding of European Union (EU) projects with international cooperation like SECRET[1], which focuses on the security of railways against electromagnetic attacks; SECUR-ED[2], a project to enhance the security of urban public transportation with work packages focused on IT security, have been carried out. Also the European Union Agency for Network and Information Security (ENISA) concentrates on developing IT security measures for the railway sector [2]. The International Union of Railways (UIC) has also started a project ARGUS with international cooperation on designing a security analysis approach for railway signaling system [3].

In Germany, the *Law of IT Security*[3] has come into effect in July 2015, which forces critical infrastructures like the railway system, whose unavailability or failure of the system could cause significant impact on the safety and living of the society, to implement adequate organizational and technical measures to avoid the complete failure or breakdown of the system. The law requires the critical infrastructure to use state of the art methods to protect the availability, integrity, authenticity and confidentiality of its IT systems [1]. Besides, in the German Commission for Electrical, Electronic & Information Technologies of DIN and VDE (DKE) two pre-standards were set up for considering the IT security threats in railway signaling: VDE V 0831-102 focuses on defining the protection profile for technical functions and VDE V 0831-104 offers an IT security guideline based on IEC 62443 for electric signaling systems in railway [4, 5].

However, all the current work in IT security, from researchers, railway undertakings, infrastructure managers to the public authorities and standard committees focusses mainly on the technical side of the railway system. The purpose of those current works is to find the vulnerabilities of today's technical system; to set up standards for technical system design; to integrate IT security management systems with the safety related

[1] *Security of Railways against Electromagnetic Attacks*, http://www.secret-project.eu.
[2] *Secured Urban Transportation – European Demonstration*, http://www.secur-ed.eu.
[3] Original in German: IT-Sicherheitsgesetz.

electronic systems, etc. However, even with all those technical measures in place, railways cannot be completely secure indefinitely. Therefore, concerns from the operational side should be considered when discussing how to deal with IT security threats, e.g.:

- What happens if the technical system fails to identify an attack?
- What happens if the technical system fails to defend against an attack?
- When and how should the operational personnel be informed about attacks?
- How can the operation be kept running safely and efficiently when the system state after a potential attack is not clear?
- How and when can operations go back to normal state, if the reasons and consequence of the attack are not completely understood?

Those questions can be summarized as: What happens when the technical measures against IT security breaches fail? Today's railway system has already shown that even technical systems with a high reliability do fail. Degraded operations are still part of operations in the daily praxis. Hence, those questions from the operational side are rational and should be seriously considered.

Network Rail has described in their IT security strategy: "We will operate in an assumed state of compromise, that is there will not be a presumption that our network boundaries, internal and external, are invulnerable" [6]. The French Network and information Security Agency (ANSSI) has considered the lack of Business Continuity Plan as a vulnerability of the industrial control system in IT security, and points out that the operation teams rarely know how to act in such IT security event [7]. In the urban transportation sector, the American Public Transportation Association (APTA) has also noticed this issue and introduces five kinds of plans that are needed for continuation of operation under the IT security threat. These plans are Incident Response Plan, Business Continuity Plan, Continuity of Operations Plan, Crisis Communications Plan and Disaster Recovery Plan [8].

3 Process of Operational Continuity

3.1 A Generic Bow-Tie Model of Operational Continuity

In Europe, the railway system has been recognized as the safest transportation mode in surface transport [9]. This achievement is built mainly on the high reliability of the system. This high reliability could not be reached without adequate operational procedures and qualified and reliable personnel. However, a system with very high reliability does not mean that no faults and no errors would occur during the system operation. As a critical infrastructure, measures and rules, both from technical and operational side, have been established in the past to achieve its high availability. Depending on the situations, measures and rules would be combined to set up procedure for the system to enable the continuation of operation.

As shown in Fig. 1, the procedures to continue railway operations can be displayed as a generic bow-tie process [10]. The process has been divided into technical and operational side, with technical on the upper side and operational on the lower side. The process begins in normal operation. With the monitoring program from one or both sides,

it leads the system from normal into degraded operation. During the degraded operation, the operational side focuses on the degraded mode management to keep the operation running; the technical side supports the operational side with the failure mode management to identify and rectify the abnormal situation. After the abnormal situation has be rectified and controlled, the transition from degraded to normal operation begins within the restoration program.

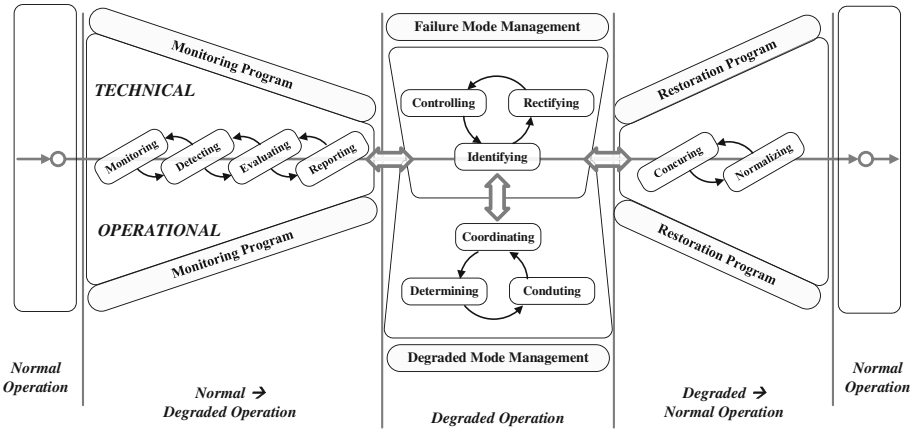

Fig. 1. General system procedure to continuation of operation in railway operation [10]

This generic bow-tie process was derived from the conventional railway procedures. The framework was set up before the issue of IT security had been considered. The question is therefore: Could this process be used when IT security has to be considered?

3.2 A Short Comparison of Safety Hazards and IT Security Threats

To decide if the model for safety can be used for IT security, a detailed analysis of the processes, relationships and dependabilities for both aspects needs to be done. As we will focus on operations, the criteria of comparison will be taken from the effects that hazards and threats might have on railway operations. The short comparison is done in Table 1. Due to page restrictions, only some chosen criteria are shown.

The comparison clearly shows that regarding its effect on operations, major differences between safety hazards and IT security threats exist. The characteristics and consequences of IT security threats are in general less well known. This means that procedures for operations in degraded mode after IT security attacks have to cover a wider set of scenarios. Therefore, we have to conclude that the procedures from today's operational rulebooks cannot be used directly to sustain operational continuity after security attack. However, we can still use them as a starting point for further research, aiming at adapting and further developing existing procedures. Based on the results shown in Table 1, we assume that today's procedures for degraded operation are a subset of the needed procedures for degraded operation in the future. Thus, the bow-tie process

Table 1. Comparison of safety hazard and IT security threats in railway operation

⁋	Safety hazards	IT security threats
1. Frequency	• Controllable – System reliability – Preventive maintenance	• Might NOT be controllable – Willingness of attacker – Purpose of attacker
2. Cause	• Foreseeable – Operation conditions – Product lifespan	• Might NOT be foreseeable – System status – Capability of attacker
3. Effect	• Predictable – System failure behavior	• Might NOT be predictable – Unexpected behavior
4. Extent of effect	• Calculable – Controlled multiple-faults – Reliable system	• Might NOT be calculable – Network-wide attack
5. Duration of effect	• Could be estimated – Failure cause foreseeable – Long-time experience	• Might NOT be estimated – System behavior unknown – Merely no experience
6. Involved persons	• Could be estimated	• Might NOT be estimated – Extent, consequence and duration unknown
7. Detection measures	• Well developed and integrated – Reliable system monitoring – Operational procedures	• Less known – Huge technical deficiency – No operational procedures
8. Time to detection	• Foreseeable – Reliable system reactions – Routine maintenance	• Might NOT be foreseeable – Unknown system behavior – Manipulation

today will still be the core framework of future degraded operation and can be adapted and developed further when IT security has to be considered (Fig. 2).

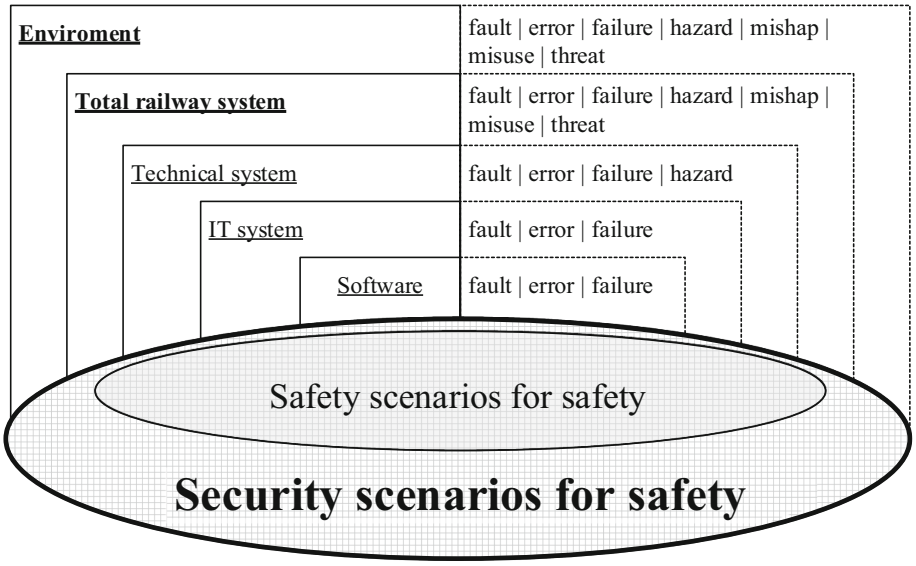

Fig. 2. Wider scenario considerations of security, adapted [11]

4 Introducing Operational Security

4.1 Scope

As previously mentioned, a modern railway system needs IT security to ensure its functional safety. This statement is correct indeed, but all the current work is only concentrated on the technical side in the railway sector. However, even though railway automation has been in process for several decades, the role of human stays indispensable in the railway operation. Therefore, a holistic view of railway operations needs to take the human into account and the effects of safety and security issues on them need to be addressed. For example, the operational personnel needs to know:

- how to identify and get aware of an attack, which was not detected with the technical measures,
- how to act during or after a successful attack,
- how the communication between operational personnel will work, e.g. regarding priorities and responsibilities and
- how to keep the operation running safely and efficiently when the status of the system is not clear.

Those requirements above are merely part of the complex set of requirements to be applied to the future railway operational procedures. Owing to the complexity and diversity of the railway operation, new approaches need to be developed to enable a systematic process to solve the problems. A new research field, which will be known as Operational Security [12], is now researching this topic intensively.

As discussed before, we assume that safety issues can be dealt with more easily because of a limited set of expected scenarios. We will include the assessment of today's rules for degraded mode in our research. Our aim is to develop a complete set of procedures to deal with safety and IT security issues. This is also necessary as we have to assume that often when an operational problem arises it cannot be decided quickly and surely if the reason for it lies in safety or security.

4.2 Essential Requirements

Before developing or adapting operational procedures, strict requirements need to be set against which the new procedures have to be proven. Identifying all requirements is still part of research, but four essential ones can already be presented as examples:

- **Operational procedures need to be safe**
  As safety is the core value of the railway system, all operational procedures need to be safe. Showing how safe is safe enough is a difficult topic.
- **Operational procedures need to be efficient**
  The operational procedures today were developed for a system with superior reliability and availability. The frequency and the duration of failures and therefore the necessity of operating in degraded mode was on a low and acceptable level. Thus, the efficiency of the procedures and the service level of the system in degraded operation was adequate to the status quo. However, the situation is changing as the

frequency, duration and also the consequences of attacks on IT can hardly be foreseen. Efficiency becomes a primary requirements for the degraded operation to keep the service level of the system acceptable as it is expected that e.g. degraded operation due to security breaches is longer in place than after typical technical failures.

- **Operational procedures need to be secure**
  The operational procedures should be secured against IT attacks. Operational procedures must not become vulnerabilities in the system. Otherwise, the attacker could force the technical system into failure mode. Since the operational side needs to take over, less secure operational procedures in the degraded operation could be exploited by the attacker. Today's operational procedures (for degraded operation) are safe but not necessarily secure, since its framework and core concept were developed in a time without the issue IT security.
- **Operational procedures need to be modular**
  Since efficiency is an essential requirement for the procedures, a modularity of procedures could be the essential point to achieve it. The operational procedures should be divided into secure procedure modules with more flexibility for interchange so that depending on the system state the modules can be chosen so that always the highest level of efficiency is possible.

4.3 Work Packages

The work of operational security can be divided into four main work packages according to the process shown in Fig. 3: Monitoring Program (WP-1), Degraded Mode Management (WP-2), Restoration Program (WP-3) and Interface Management (WP-4). Additionally, two further work packages are need. One will look at the state of the art in degraded operation and will derive a full set of requirements (WP-5). Another one will deal with the basic ontology to represent the intended meaning and relations of terms which to be used in operational security. (WP-6). The work packages are described below to give a first overview about the expected research efforts.

- **WP-1: Monitoring Program**
  The operational monitoring program begins with defining specific events which the operational personnel should be aware of in the running operation. Measures of how to detect and reveal those events will be integrated into procedures of normal operation. Criteria to evaluate the threat level of the detected events will then be set up to help the operational personnel to make decisions and to assess the potential consequences swiftly in the running operation. Regardless of whether the detected events could be instantly classified as threat or not, the events should be reported to the responsible person or unit in a defined process for further assessment. It will be defined which information of the given operational situation will be used as benchmarks for choosing the appropriate degraded mode operation and where to get those information from.
- **WP-2: Degraded Mode Management**
  The degraded mode management can be considered as a set of systematically defined procedures, which should be put into action immediately to ensure the operational

continuity after the detected event has been reported. Responsible persons for coordinating, determining and conducting the degraded mode operations will be defined. The communication process between operational personnel, criteria for determining proper countermeasures and priority of procedures will be established.

- **WP-3: Restoration Program**
  The restoration program focuses on procedures to bring the system from degraded operation back to the normal operation. After the detected event has been rectified and controlled from the technical side, the system status need to be concurred between technical and operational personnel before return to the normal operational procedures. Detailed processes and responsibilities are needed.
- **WP-4: Interface Management**
  There are interfaces between the phases of operations as well as between operational personnel and technical management. These interfaces will be clearly defined and the necessary information at interfaces are identified. It will furthermore be discussed how inaccuracies or missing information will invalidate the processes. It must be the aim of the whole setup to be stable and not lead to wrong conclusions when minor inaccuracies exist.
- **WP-5: Requirements**
  New operational rules have to take into account the requirements put on them by legal documents. Further requirements come from operations itself. Additionally, as

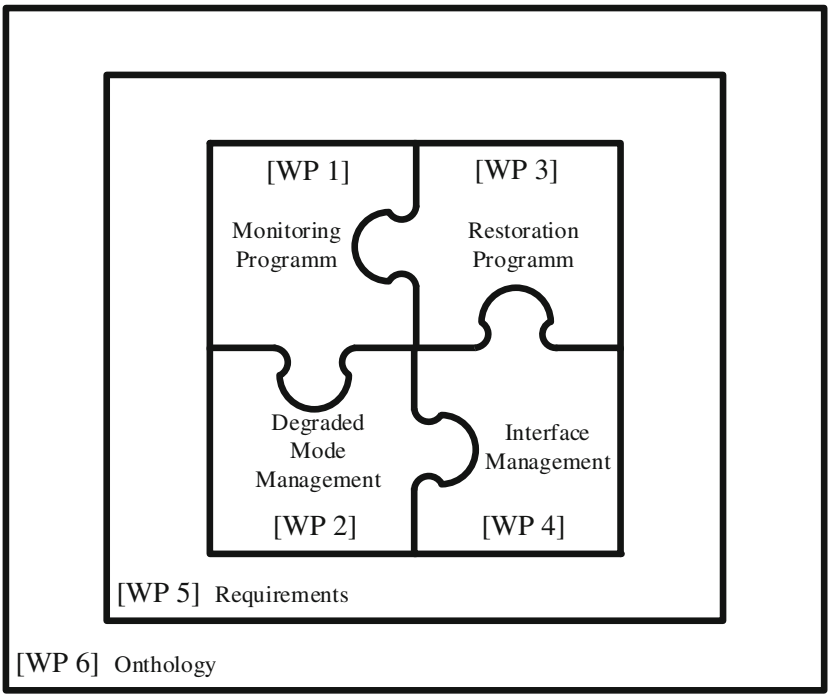

Fig. 3. Work package set-up

railways are very complex and difficult to change, they should be based on today's rules as these are known and accepted. The aim of this work package is to derive a complete set of requirements which the new rules have to adhere to. This will allow to check if and which existing rules will still work, but it can also be used as a benchmark to check if a new set of rules is feasible.

- **WP-6: Definitions**
  As security is a rather new topic, today's definitions are not completely usable in the context of operational security. An ontology is needed to merge, define and connect definitions and relationships which were established for safety with the ones used for security.

5 Conclusions and Further Works

This paper has shown the importance of operational continuity in railway operations under IT security threats. It was revealed that in the current work regarding IT security in the railway sector this aspect is not taken care of. A new research field named Operational Security has been introduced. Operational security aims at systematically developing a closed set of operational rules for dealing with suspected or actual IT security breaches. It was argued using some examples that today's rules for operations in degraded operation are not completely suitable as they were developed mainly for safety issues. On the other hand, we have to take into account that distinguishing between safety and security irregularities will not always be possible. It is an aim for operational security that the developed rules are applicable to safety as well as security issues. In the paper, we suggest a plan for researching operational security and discuss the main work packages and give an overview of what to focus on in each.

References

1. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, Bonn (2015)
2. Lèvy, C.-B.: Cyber security for railway signalling (presentation). In: Workshop on "How to Protect Signalling System Against Cybercrime," Paris (2015)
3. Antoni, M.: ARGUS – Security & safety analysis for electric and computerized signalling systems (presentation). In: DKE Meeting 2014, Frankfurt (2014)
4. DIN VDE V 0831-102 Electric signalling systems for railways - part 102: protection profile for technical functions in railway signalling (2013)
5. DIN VDE V 0831-104 Electric signalling systems for railways - part 104: IT Security Guideline based on IEC 62443. (2015)
6. Cyber Security Strategy. Network Rail, London (2013)
7. Cybersecurity for Industrial Control Systems – Detailed Measures. The French Network and Security Agency (ANSSI), Paris (2014)
8. APTA: Cybersecurity Considerations for Public Transit. APTA (American Public Transportation Association), USA (2014)
9. Railway safety performance in the European Union 2014. European Railway Agency, Valenciennes (2014)

10. Huang, P.-C., Milius, B.: IT-Security für einen sicheren Bahnbetrieb. Deine Bahn. 2/2016, 13–16 (2016)
11. Raspotnig, C., Opdahl, A.: Comparing risk identification techniques for safety and security requirements. J. Syst. Softw. **86**, 1124–1151 (2013)
12. Huang, P.-C., Milius, B.: Why do we need operational security? (presentation). In: 8th Workshop on "Safety in Transportation," Braunschweig (2015)