Huang Po-Chi
Technische Universität Braunschweig, Braunschweig, Germany

A multipurpose generic framework for developing systematic railway operational rules

Keywords

railway operation, IT security threat, operational rules, degraded operation, railway safety, functional safety

Abstract

Typically, railways have developed over time. When new technical system became available, they were adapted and integrated into the existing system. Usually, this led also to adapted or changed operational rules. However, there was never a structured and systematic approach in the development of operational rules, at least not in Germany. It is very difficult to get a comprehensive overview of today's rules and also to estimate and compare the effect of significant changes. One of these concrete significant changes is the necessity to hardening railway operations against possible IT security threats in modern railway IT systems. We realized that, in order to have an approach which can evaluate, adapt, develop, trace and manage the operational rules systematically, a new multipurpose generic framework will be needed. In this paper, we focus on introducing a multipurpose generic framework and its usage for developing systematic railway operational rules. The work in this paper is part of our ongoing research project SysRULES (2017-2019), which is funded by the Karl Vossloh-Stiftung in Germany.

1. Motivation

In July 2015, the German IT Security Act has become legally binding for critical infrastructures, like the German railways and the railway industry. The IT Security Act requires in §8a (1): "Operators of critical infrastructures are obliged to [...] take appropriate organizational and technical precautions to prevent disruption of the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes which are crucial for the functioning of the critical infrastructures they operate." [4]

The main work of today's railway IT security activities is focused on eliciting requirements and developing an IT security management system, which, in simplified terms, deals with the collection and analysis of data. Another focus of the work is the system design, for example the derivation of structures and architectures, which should make new systems and communication structures as secure as possible. The goal of all work in this area is to develop and maintain systems so that attacks are possibly recognized and prevented.

However, we still need to realize that even with the best IT protection, there might and probably will be an incident in the system [3]. The lack of the business continuity plan has been recognized as a vulnerability in the industrial control system under the threat of IT security [1]. In railway area, the continuity of operations after an IT security attack or a suspected attack is also not part of the ongoing research. At the most, it is stated that it is necessary, without giving further details. Otherwise, there exist no detailed instructions in the most business continuity plan for the first line operational staff of how to use the detailed safety-related operational rules under the threat or breach of IT attack.

Modern railway systems usually have the degraded operation modes to ensure their continuity of operation. However, today's rules for degraded operations were barely developed in a systematically manner, not to say under consideration of IT security. As of today, there are no rules which apply especially to security breaches. If something is wrong, the same rules as for "regular" problems will be applied. We cannot assume that today's rules will allow an acceptable level of safety and punctuality in degraded mode after a functional failure due to IT security breaches.

However, having two sets of rules, one for safety and one for IT security, would make it difficult and complex for the operational staff to choose the correct one. As we have to take into account that it is not

always obvious from beginning, if an event is safety or IT security related. A survey in 2016 shows that a company needs in average 49 days [12] or 99 days [9] to realize that their system is the victim of an IT security attack. Therefore, we argue that, for the degraded mode of the critical infrastructure like the railway system, a set of operational rules which could deal with safety and IT security issues concurrently will be needed, especially when the overall system state is unclear.

2. Systematic Rules for Railway Operations

2.1 Project SysRULES

The work in this paper is part of our ongoing research project SysRULES (Systematic Rules for Railway Operations), which is funded by the Karl Vossloh-Stiftung in Germany. The authors were granted this three years project (2017-2019) to develop concepts for railway operation in degraded mode due to the IT security threats. The proposed project has a total of 7 work packages (WP) as shown in *Figure 1*. For more details of the project packages please see [6]. The scope of this project focuses strictly on the operating part of railways and how IT security threats and breaches might influence railway operations. The goal of this project is to develop a generic set of structured and systematic operational rules, especially for train dispatchers (in the following "dispatcher"), that is to be used in degraded mode after potential or successful IT security attacks.

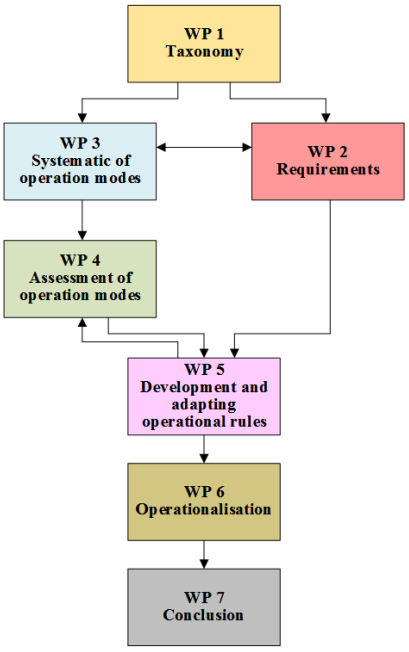

Figure 1. Work packages and outline

The approach of this project can be divided mainly into two stages. In the first stage, we assume that by an IT attack, even though it is not clear if it is safety or security related, the implemented technical protection measures should be able to divert the system into a fail-safe status, which resulted in the use of degraded mode. Due to the steady increase in IT security attacks in the last few decades, we argue that the railway system will need to run operations in degraded mode more frequently. Even if the reliability of these processes stays the same, this will lead to an overall increase in the number of safety-related events and therefore also an increase in the associated risk of using the existing operational rules in degraded operation. Moreover, the task of the operational staff get more and more passive due to the automation of the railway operation. In cases where the dispatcher needs to interact with the operation, the passiveness of dispatchers and therefore a reduced situation awareness could also cause a higher risk in operation [7]. The target of this stage is to analyse and adapt the existing rules and to make the use of existing degraded modes safer and even efficient.

In the second stage, we argue that the attacker could select the less protected degraded mode as attack target. The degraded mode should also be reasonably protected against IT security attack accordingly. We will take the adapted operational rules from the first stage as input, to analyse the degraded mode again with using IT attack vectors to understand the effect and its related risk. We will once again adapt and develop new rules to make the operation in degraded mode reasonably safe and secure accordingly. At the end, a set of operational rules for the degraded operation which could deal with safety and IT security issues concurrently will be developed.

However, as stated before, there was never a structured and systematic approach in the development of operational rules. It is very difficult to get a comprehensive overview of today's rules and also to estimate and compare the effect of significant changes. We argue that, in order to have an approach which can evaluate, adapt, develop, trace and manage the operational rules systematically, a new multipurpose generic framework will be needed as a basis. Therefore, in this paper, we focus on introducing a multipurpose generic framework and its usage for realizing systematic railway operational rules. However, the analysis of the operational rules according to safety related event or IT security attack is not in scope of this paper.

2.2 General scope of operational rules

The operational rules in Germany are published as part of the network statement from the infrastructure manager DB Netz AG. Due to the organizational separation of railway undertaking and infrastructure manager in Germany, the publicly accessible

operational rules today contain only rules, which are relevant to the staff of railway undertakings to run the operation in the infrastructure. The "rule books for dispatcher", officially known as "Fahrdienstvorschrift" in German, is formally not part of the publicly accessible network statement, but still publicly available for understating the railway operation as a whole.

Formally, the rule book for dispatchers has been divided into "Rule book for train running" (408.01-06) and "Rule book for train shunting" (408.48) according to its usage in operation. The rule book contains generally only those rules, which are valid on the standard infrastructure and system design. Specific rules due to local exceptions that are only valid in certain operating locations are not the content of this rule book. Those specific rules are documented individually in the rule book of the relevant locations. The rule book in Germany has a function-based structure. Rule books with this structure have the advantage that the operational rules can be documented in a very compact form. More alternative measures and events could be documented in the same number of pages in compare with process-based structure [10].

Regarding content of the rule book for dispatcher, the basic content of the rule book is the general functional safety logic and philosophy of the operation. Furthermore, according to the events identified, the rules books contain the rules of using certain degraded modes to realize certain desired function. The degraded mode can be understood as an alternative path to achieve the same objectives as in the normal operation [7]. Therefore, the use of a certain degraded mode in operation has mostly to be in combination with or based on certain rules which contain the general functional safety logic and philosophy of the desired function.

According to our preliminary analysis in our project, the existing degraded modes could be generally sorted into four categories based on its time point of use, staff involvement and the duration of use as shown in *Table 1*. These four categories are: planned measure, automated measure, short-term measure and temporary measure.

The category planned measure contains those degraded modes, which have a planned time point of use, ex. during the construction work, maintenance work, or hurricane. For those degraded modes, the time point of event happened is certainly known, therefore the time point of the use of degraded mode could be planned beforehand. Since those events will usually affect the operation for a certain time, the duration of use the planned degraded mode could last from days to even months respectively.

The category automated measure contains those degraded modes which have been widely solved automatically with ex. technical redundancy, whether the event happened as expected or randomly. The use of this degraded mode will be triggered automatically usually without observable delay once the event happened. Commonly, this kind of degraded mode has been widely considered as normal operation and as part of the normal system design. Therefore, the automated degraded mode is generally not included in the rule books and will not be further discussed in this paper.

The last two categories: short-term measure and temporary measure differ mainly in its duration of use. Both are degraded modes used when the event happened randomly during the operation. The short-term measures are usually one-time or few-times measures to deal with the short time event, ex. clearance check in block section for a single train, emergency stop. On the opposite, the duration of using temporary measures could last to several hours to days, ex. clearance check in block section for a duration of time.

Table 1. General category of degraded modes

Degraded Mode				
Time point of use is	Expected		Random	
Planning horizon	Planned before event happened		Made swiftly after events happened	
Category	Planned measure	Automated measure	Short-term measure	Temporary measure
Staff involved	Yes	No	Yes	Yes
Time to begin	Middle to Long	No observable delay	Short	Short to Middle
Duration of use	Middle to Long	Short to Middle	Short	Short to Middle
Example	operation under construction work	technical redundancy	Clearance check for a single train	Clearance check for a duration of time

2.3 General problematic of existing rules

Over the years, the function-based structure of the rule book has not been changed much. However, the content of the rule books has increased with time, but without a systematic approach as basis. For example, when new technical systems have been implemented, new events have been identified or new measures have been developed after an accident, rules were adapted or added to the chapter of the corresponding function or event accordingly. This approach of adapting rule books over time has made today's rules very complex and makes it hard to evaluate the rules systematically.

The problematics of existing rule structure could be summarized as follows:

Complex or unneeded information
In the function-based structure, rules of degraded mode to deal with a certain identified event and/or to realize a desired function are sorted together according to the event or to the function. However, when new technical systems / new methods have been implemented, rules relating to the degraded mode of the new implementation have usually been added to the existing chapter or paragraph directly. This approach indeed makes the rule book very compact, because all the rules of different technical or methodical implementation which related to the same event or function could be collected together. However, over the years, this approach makes the rule book very complex in its logic and contains certain unneeded information for dispatchers who only need those rules for certain system(s) in their control area(s). Safety related rules shall be direct, clear, without ambiguity. The mixed logic of complex rules and the unneeded information could cause ambiguity in use.

Missing of process linkage
In comparison with the process-based rule book, the inherent disadvantage of the function-based rule book is its missing of direct process linkage among actions. To enable a process after an event happened, ex.: train running movement when signal failed to show proceed, the dispatchers need to select, decide and connect the valid actions from the rules of the degraded mode and the general basic logic, which are usually documented in different chapters with very complex, less intuitive or even none cross-references among each actions. The missing of clear linkage might not be an issue for a rule book which only contains single system logic and implementation. However, as stated above, the content of the rule book has become complex over time and the missing of linkage causes usually ambiguity when selecting and applying rules.

Missing of systematic approach
The existing rules were never developed, adapted or managed by using a well-structured method. As stated above, when ex. new technical systems are implemented or accidents happened, new rules will be added to the belonging event or function or existing rules will be adapted. Today's approach does not allow a systematic development, evaluation, management and innovation of operational rules. Moreover, with the missing of a systematic approach, the traceability of the rules is not guaranteed. Once a rule has been adapted, it is hard to trace the origin or even understand the background of the rules after years. We argue that the rule book should not be a history book with a rich collection of experience from the accident. On the contrary, the modern rule book should have a systematic structure with traceable logic which also enables an integrated development, assessment, evaluation, management or even modelling and simulation of the operational rules.

Missing of quality statement
The effect of existing rules on the quality of operation, ex. the associated risk, is accepted as it is over years. The information about the associated quality is until today not part of the existing rule books. The missing of the quality statement might not be an issue if only accidental or unintended events are considered as cause of degraded mode. However, with considering that the railway system has been classified as critical infrastructure and the effect of IT security attack could get wider and last longer [5], more quality statements like associated risk, operation performance, and strain on dispatchers could be generally included in the rule books to set up priority for choosing appropriate degraded modes in operation under the threat or breach of IT attack.

Missing of interactive use
Along with the development of the railway system over time, the dispatcher today has usually rule books with at least several hundred pages for use. The existing rules are written in natural language with normally a paper-based documentation. Even with the digitalization of the rule book and using new technology nowadays, the existing rule book with text-based structure does not enable an advanced interactive use of operational rules directly. However, the paper-based operational rules have their limit and do not allow to express a complex systematic method which contains the ex. process, traceability, assessment, etc. in a clear and comprehensible way. Inevitably, a software-based solution will be needed to host such a complex systematic method and to realize a further automation of degraded operation through ex. interactive use of operational rules between dispatcher and software.

3. The multipurpose generic framework

3.1 General concept and structure

After understanding the general scope and the problematic of the existing rules, we've realized that the vast amount of information and also the complexity of the information which we are facing, have widely exceeded the ability that a paper-based documentation could handle. Therefore, we argue that the new solution shall have a systematically defined and layered structure which could be further

transformed into a software-solution without great effort. Moreover, as the model-based system design and software development have become the state of the art in the engineering domain, we've decided to have a solution which shall also allow the modelling of the process of operational rules using widely used graphical modelling language like SysML/UML. As a holistic solution for the known problematic of the existing rules (*Figure 2*), we introduce here a multipurpose generic framework which contains a well-founded structure and is able to realize a traceable and systematic development, assessment, evaluation, adaptation, innovation and management of the operational rules.

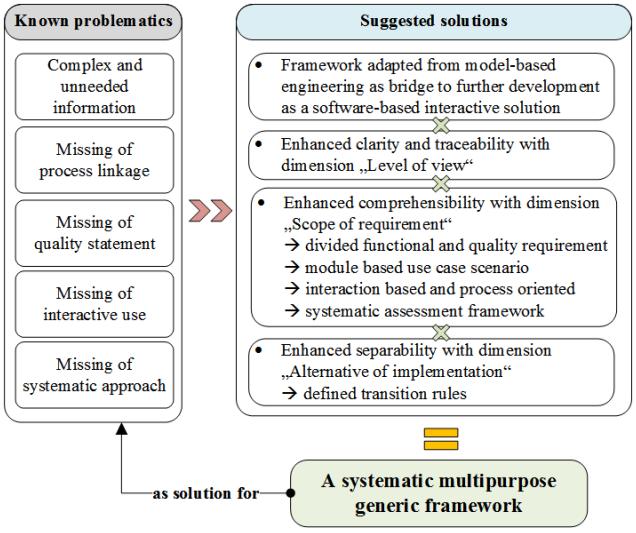

Figure 2. Problematics and suggested solutions

However, before we go further to introduce the general structure of the proposed generic framework, we need to emphasize that the purpose of this framework is not to model or to develop the whole systems. The framework was planned to reorganize and to systematize the operational rules at first. The following multipurpose generic framework is a further development of our initial concept and it could be further developed as an assistance system for the dispatcher in cases where the rules need to be used in the operation.

In order to solve the problematic with complex and unneeded information, missing of process linkage and quality statement, we purpose a three dimensional structure to set up the framework. These three dimensions are: "level of view", "scope of requirement" and "alternative of implementation". In brief, the dimension "level of view" is used to realize an enhanced clarity and traceability of the operational rules; the dimension "scope of requirement" is to improve the comprehensibility of the requirements and the process; the last dimension "alternative of implementation" has the ability to separate the different implementations and contains the defined transition rules. Note that even though each dimension has its own purpose, it cannot be taken apart from the framework to be used alone.

3.2 Dimension: level of view

The first problematic that we have realized by analysing the existing rules is its complex and unneeded information. With using the dimension "level of view", we try to divide the information into different layers according to the depth of the information. We've defined three levels of view in our framework, they are: "Generic level", "Transformational level" and "System-specific level" respectively (*Figure 3*).

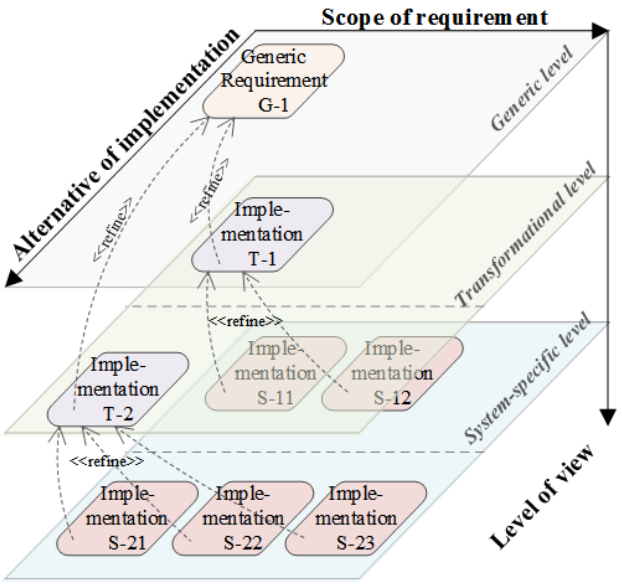

Figure 3. Structure of the generic framework

The dimension level of view alone does not have much use, but when in combination with the other two dimensions, we can achieve a connection of generic requirements and alternative implementations from generic to system-specific as shown in *Figure 3*. Note that in order to achieve the traceability between requirement and implementations, we defined that an implementation at a higher level (ex. transformational level) will be the requirements of the implementations at the lower level (ex. system-specific level) at the same time. Or we could also say that the implementation at a lower level is to refine the requirement at a higher level. Details of the requirements and implementations will be further explained in the following paragraphs.

3.3 Dimension: scope of requirement

As we realized the problematic of missing process linkage in the existing rules, we have also become aware that the use of degraded mode has mostly be

based on or in combination with the default safety logic. Otherwise, from the view of requirement, the degraded mode could be understood as an alternative implementation to achieve the same functional requirement as in the normal operation. We argue that the way to have a systematic approach to understand the degraded mode needs to begin with knowing the desired requirements and its general default logic process in normal operation.

Commonly, the requirements could be divided into functional requirements and quality requirements [11]. As the functional requirements state "what" the system shall do, the quality requirement concentrate on "how good" a function shall achieve its goal. Considering that one of our use of this framework is to evaluate the quality of different degraded modes, we decided to adopt the separation of functional requirement and quality requirement in our framework. Talking about the quality evaluation, the framework offers merely a structure as placeholder for the quality requirements. In order to have a better adaptability of using different evaluation methods, especially when multiple quality criteria evaluations are needed, we decided not to integrate any default evaluation method into this framework.

Since a function is an ability of a system to be operated under certain conditions, a function alone does not mean much for the dispatcher. Therefore, the description of the functional requirements should also contain its surroundings. In order to include the surroundings in the description of the functional requirement, we use the module-based structure to describe the generic functional requirements as use case scenario in the generic level. This module-based structure offers a great adaptability for the user to construct the generic functional requirements into certain details as needed.

In *Table 2*, we show an example of the generic functional requirement as use case scenario: "*Realizing train separation for train running movement in successive direction though area with track only in block section under normal wetter*". This use case scenario is constructed through the combination of the selected parameter(s) from six basic modules. Note that the framework does not specify the content, detail or number of the modules or parameters to be included. The main restriction is that the description of the functional requirement needs to be generic. It means that no process logic, interaction or implementation are allowed in the description of this level.

Table 2. Generic functional requirement as use case scenario (example, not exhaustive)

	Module	Parameters
1	Function (Realizing train…)	- train separation - train control
2	Type of movement (for … movement)	- train running - train shunting
3	Direction of movement (In … direction)	- successive - opposing
4	Infrastructure element (Through area with…)	- track only - movable track element - crossing
5	Operation area (in … area)	- block section - station area
6	System environment (under…condition)	- Normal wetter - Hurricane - Construction
Use case scenario though combination of modules: (1/realizing train separation)*(2/for train running movement)*(3-in successive direction)*(4/though area with track only)*(5/in block section)*(6/under normal wetter)		

From the generic level, we go deeper to the transformational level and system-specific level. As the generic level contains the general requirement of the system, the transformational level and system-specific level refine the general requirement with implementations. As shown in Figure 3, each implementation in the transformational level is allocated to a certain functional requirement which described as use case scenario in the generic level; also each implementation in the system-specific level need to be allocated to a certain implementation at the transformational level.

To solve the problematic of the missing process linkage in the existing rules, we use an interaction based and process oriented systematic to describe the implementation in both transformational and system-specific level. This systematic was adapted from the structure of a human centred mapping framework for layered degraded modes from Huang & Milius [7]-[8]. Their systematic uses the concept of control nodes (see also concept of control node in systems modelling language SysML/UML [2]) to represent single process steps generally. At each control node, there exist a control rule which shall be achieved through an actor-entity based interaction. The simplified process view of an implementation can be constructed by lining up the control nodes chronologically, like a dispatcher will perform a sequence of control interactions to realize a use case scenario when using the operational rules. Moreover, the simplified process has a fixed first person view as default view point. It means that in our case, the dispatcher will always has the role as "actor" in the relationship, except when the computer takes over the role of dispatcher, like in the automated normal operation.

In our paper, we have adapted this systematic and merged it further into our framework with the three

dimensions introduced. In *Figure 4*, we show an example of using the systematic to describe an implementation as simplified control process at the transformational level for the use case scenario described in *Table 2*.

Use case scenario G-1: (1/realizing train separation)*(2/for train running movement)*(3-in successive direction)* (4/though area with track only)*(5/in block section)*(6/under normal wetter)				
Transformational level: implementaion M-1 Assumptions / initial conditions: - logical decision of train separation made by Key-Actor - Key-Actor is outside of the train - Key-Actor does not have active control over the train movement - entering the successive block area is strictly not allowed without movement authority				
Sequence of Controls				Control rules
I1	Key-Actor	<--->	Entity	to ensure the clearance of the train path through the area (n) to the overlap subsequent
I2	Key-Actor	<--->	Entity	to ensure the train path from the area to the overlap subsequent has been set
I3	Key-Actor	<--->	Entity	to ensure the movement authority to train for entering the area has been issued
I4	Key-Actor	<--->	Entity	to ensure the train has entering the area
I5	Key-Actor	<--->	Entity	to ensure the train has been protected against following movement
I6	Key-Actor	<--->	Entity	to ensure the clearance of the train path through the area (n+1) to the overlap subsequent
I7	Key-Actor	<--->	Entity	to ensure the train path from the area (n+1) to the overlap subsequent has been set
I8	Key-Actor	<--->	Entity	to ensure the movement authority to train for entering the area (n+1) has been issued
I9	Key-Actor	<--->	Entity	to ensure the train has entering the area (n+1)
I10	Key-Actor	<--->	Entity	to ensure the clearance of the train path through the area (n) to the overlap subsequent
I11	Key-Actor	<--->	Entity	to ensure the train path through the area (n) to the overlap subsequent has been released

Figure 4. Example of implementation at the transformational level for use case scenario in *Table 2*

The main difference between the description of transformational level and system-specific level is the following: the actor and the entity in the transformational level is not named. The transformational level should only contain the generic process logic to realize the use case scenario from the generic level "without knowing who is who". Even the description of the control rules should not contain any system-specific solution. For example, an actor (ex. dispatcher) could interact with an entity (ex. way-side signal, cab-signal, written order, etc.) to issue the movement authority to the train. In the transformational level, all we know is that at a certain process step, an actor needs to interact with an entity to issue a movement authority to the train. The use of way-side signal, cab-signal or written order are all the implementations at the system-specific level. Moreover, according to the use of different system-specific implementations, different level of quality ex. risk, speed, performance could be evaluated. However, there are some more details about the regulations and constraints of using the systematic to describe the implementations. Since the purpose of this paper is introducing the whole concept of the framework, the details of the systematic will not be further discussed at this point.

Another advantage of using this systematic to describe the implementations is that there exists a structured interface to the existing FMECA oriented risk assessment framework as described in [7]-[8]. This existing risk assessment framework has a systematic approach to derive and evaluate the failure mode from the interaction based simplified process. According to the identified failure mode, the use of certain degraded mode will be needed. We will discuss about the failure mode and the degraded modes in details in the following paragraph about the last dimension "alternative of implementation"

3.4 Dimension: alternative of implementation

As we know that the degraded mode is an alternative path to realize the same objectives as in the normal operation, we argue that: for each generic use case scenario, there exist an undefined number of transformational solutions; also for each transformational solution there exist an undefined number of systematic-specific solutions. Based on this concept, we defined the third dimension "alternative of implementation" to enable a systematic separation and organizing of the implementations with different logics or systems used. This dimension is not only a placeholder for all the possible variations of normal and degraded implementations. On the contrary, this dimension also contains the important transition rules, which are used to trigger an active transition between different implementations in different levels.

In our concept, the use of certain degraded modes in operation is logically connected to the event identified. An event is a deviated state from a planned standard process, which is the cause of using certain alternative implementation in our definition. Moreover, the term event has a broader perspective which also contains the change of system surroundings, as the term failure mode usually related only to the technical system or staff considered.

Generally, the transition rules could be divided into two categories. The first category contains those rules for direct transitions after an event is identified. They are the transition rules of entering or shifting between short-term measures which like categorized in Table 1, ex. shift between alternative interactions, same or different level implementations. The second category contains those rules for transitions due to quality consideration. They are used to decide which category of degraded mode (see Table 1, planned, short-term or temporary measure) should be used according to the consideration of the operation quality. For example, they are to decide how many times a short-term measures should be used before change to temporary measure; or when an identified event has reached a certain extent and the use of temporary or planned measure is needed directly.

Compared to the rules defined in origin of the description systematic in [7], the mapping framework does not have the three dimensional structure as our framework to hold the implementations separately. Therefore, they use the rule of alternatives and rule of transition to indicate the available implementations and its logical process connection between interactions in one compressed two dimensional framework. The mapping framework can be

considered as a compressed view of all the systematic-specific implementations of a certain transformational implementation in a process oriented structure. In our framework, we expand and reorganizing the concept rule of alternatives into containing the connection to other transformational implementations and considering the quality of implementation. The rule of transition which contains the logical process has been structurally contained in each process-oriented implementations in our framework.

4. Conclusion

Due to the steady increase in IT security attacks in the last few decades, we argue that the railway system will need to run operations in degraded mode more frequently and the degraded mode should also be reasonably protected against IT security attack accordingly. Since there was never a structured and systematic approach in the development of operational rules for dispatcher in Germany. It is very difficult to get a comprehensive overview of today's rules and also to estimate and to compare the effect of significant changes.

This paper begins by discussing the general scope and identifying the problematic of the existing operational rules for dispatcher in Germany. As solution, this paper presents the concept of a multipurpose generic framework which contains a well-founded structure and is able to realize a traceable and systematic development, assessment, evaluation, adaptation, innovation and management of the operational rules. Moreover, this framework has a structure which allows the modelling of the process using widely used graphical modelling language and could be further transformed into a software-solution without great effort.

Due to the page limit, we focus in this paper on introducing the general concept of this multipurpose generic framework. Examples of using this framework to develop the operational rules are not in scope of this paper and will be published in the following project related publications. The work in this paper is part of our ongoing research project SysRULES (2017-2019), which is funded by the Karl Vossloh-Stiftung in Germany to develop concepts for railway operation in degraded mode due to the IT security threats.

References

[1] ANSSI - The French Network and Security Agency (2014). Cybersecurity for Industrial Control Systems – Detailed Measures. Paris, France.

[2] Delligatti, L. (2014). *SysML distilled: a brief guide to the systems modelling language*. Pearson Education, Inc., New Jersey.

[3] Edwards, M. (2017). Automation (in)Security. Presentation at the Congress IT meets Industry 2017, September 19-20, 2017. Frankenthal, Germany.

[4] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (2015). Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, Bonn.

[5] Huang, P. C. & Milius, B. (2016). Operational Security – A coming evolution of railway operational procedures under the IT security threat. *Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification, International Conference Proceedings*, Springer International Publishing, 69-78.

[6] Huang, P. C. & Milius, B. (2017). A roadmap to a safer railway: How the IT security threat will influence the way we handle railway operations in the future. *Safety and Reliability – Theory and Applications, 27th European Safety and Reliability Conference*, CRC Press Taylor & Francis Group, London, 1779-1786.

[7] Huang, P. C. & Milius, B. (2017). Adapting operational rules for degraded mode based on a human centred risk assessment. *Proceedings of the Sixth International Rail Human Factors Conference*, 428-438.

[8] Milius, B. & Huang, P. C. (2017). Sichere Rückfallebenen in Zeiten der Rail-IT-Automation. *Der Eisenbahningenieur*, Heft 11, 36-39.

[9] M-Trends (2017). https://www.fireeye.com/

[10] Pachl, J. (2017). *Block and Interlocking Principles*. Lecture notes, Braunschweig

[11] Pohl, K. (2010). *Requirements Engineering*. Springer-Verlag Berlin Heidelberg

[12] Trustwave global security report (2017). https://www.trustwave.com