Adapting operational rules for degraded mode based on a human centred risk assessment

Po-Chi HUANG, Birgit MILIUS

Technische Universität Braunschweig, Germany

Abstract. Due to the increase in IT attacks, the train operator will need to run railway operations in degraded mode more frequently. This will lead to an overall increase in the number of safety-related events and therefore also an increase in the associated risk. In this paper, we use a human centred risk assessment to evaluate how safe and reliable our existing procedures for degraded mode are.

Keywords. Railway operational rules, degraded mode, systematic rules, safety, IT security.

1. Motivation[1]

The railway system is constantly changing. During the last years, this meant that more and more technical systems are introduced. The tasks of, e.g. the train control operator get more and more passive. They are monitoring operations and are only interacting with operations when special requests are done or something goes wrong.

As we do know, not the least from Bainbridge's famous paper (Bainbridge (1983)), humans are rather bad at monitoring and fall out of the loop. This means that in cases where they do have to interact, information might be missing and the situation awareness is not as good as it supposed to be. In these situations, the people are confronted with a rather complex set of rules and regulations about how to deal with problems in operations. In contrast to the technical systems, the rule book did not change much over the last years. Rather than adapting the book as a whole, new rules were introduced when new system had changed requirements on the people or when an accident happened and the old rules had to be adapted.

As a result, the German railway operating rules are an event-based, complex collection which has developed over decades. A recent accident (Bad Aibling) has shown that the application of these rules in degraded mode is difficult and prone for errors. These facts alone make it obvious that for a continuing high level of safety, it will be necessary to evaluate today's rules for degraded mode and adapt and change them to make them more easy to apply, to introduce new safety layers and therefore to reduce the error probability.

Another aspect which needs to be taken into account is the constant and raising threat from IT security breaches. 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. In general, this is not a bad idea and may work, but we have to check that all possible scenarios can be covered by existing rules. That will be a major research area for the future. Furthermore, we have to look at the risk associated with degraded mode. For the last

[1] The work on this topic is financed by the Vossloh research grant 2017.

centuries, the railway system has developed gradually. The risk associated with operations is accepted as such. This is true for normal operations as well as operations in degraded mode.

However, as Pachl (2004), pointed out in his paper, more events are likely to happen in degraded mode than in regular operation. This means that there is already a higher risk associated with degraded mode. With IT security breaches, we now have a new situation in which operations will happen in degraded mode. It will be additionally to the existing situations and means that we will go into degraded mode more often – every time a security breach is proven or suspected. Also, as less experience with IT security exists, we have to assume that it will take longer to return to regular operations – the system will be operated in degraded mode longer, raising the risk and probably putting strains on the systems performance as well as on the people controlling the system. The area which is affected by degraded mode might get bigger as IT security breaches can affect larger areas. We cannot be sure how the situation regarding IT security will develop in the coming years. However, as we know that developing rules and introducing them is a long process, the rules need to be evaluated and adapted now.

We propose the following steps:

- Reorganizing today's degraded modes into a layered structure as a basis to enable a comparison between different degraded modes.
- Assessment of today's rules; identifying possibilities for reducing the risk by adapting existing rules.
- Application of the adapted rules to suspected IT security scenarios; evaluating and adapting rules so that safety and security requirements are met
- Analysis of IT security breaches to identify scenarios which cannot be handled by today's rules; development of new rules

In the following paragraphs of this paper, we begin with introducing two frameworks which can be used together to analyze the operational modes in a very structured and systematic way. The first one is a process-based "mapping framework", which is composed of actor-entity interactions and generic control nodes. This mapping framework can be used to allocate today's degraded mode into a layered structure from both process and human viewpoint, and is the preparatory work essential for the second framework. The second one is a "risk assessment framework" using the content of the mapping framework as input. This assessment framework can be used to compare the risk when using different operational modes to achieve the same functional requirement. To demonstrate our frameworks, we use the process of ensuring train separation against following movement (Clearance check, "Räumungsprüfung") from the German operational rules. In the last part of this paper, we discuss the effect of the IT security threat on our proposed framework.

2. The frameworks

2.1 Relations between operational methods, modes and rules

Before we introduce both frameworks more thoroughly in the following paragraphs, we first need to define the context of three terms used in this paper: they are operational method, operational mode and operational rules, respectively. In our framework, an *operational method* describes a full-featured process at a higher level with particular implementation to fulfil a certain safety objective in operation, ex. train operation with automatic block system, train operation with telephone block system. There exist usually a number of operational modes in an operational method. The *operational mode* is sub-process of an operational method and can be further divided into mode for normal operation and mode for degraded operation, also known as degraded mode. The degraded mode is an alternative path to achieve the same objective as in the normal operation. For example, if a train operator failed to set the signal to “Clear”, then he can use the “auxiliary signal” as degraded mode to give the train driver the authority to pass the signal at “Danger”. The last term *operational rules* describes the regulations, which will be needed to regulate the process, the use of operational modes and other relevant activities.

2.2 Concept of using a generic framework as reference basis

Our concept of using a generic framework as basis to compare the risk of different operational modes is originating from (Huang (2016)). He used generic basic activities, which were derived from the generic safety objective of railway operations, to set up a reference process for comparison, see Figure 1. He argued that the risk between different operational methods can be compared, because their activities in the process originated from the same generic basic activities.

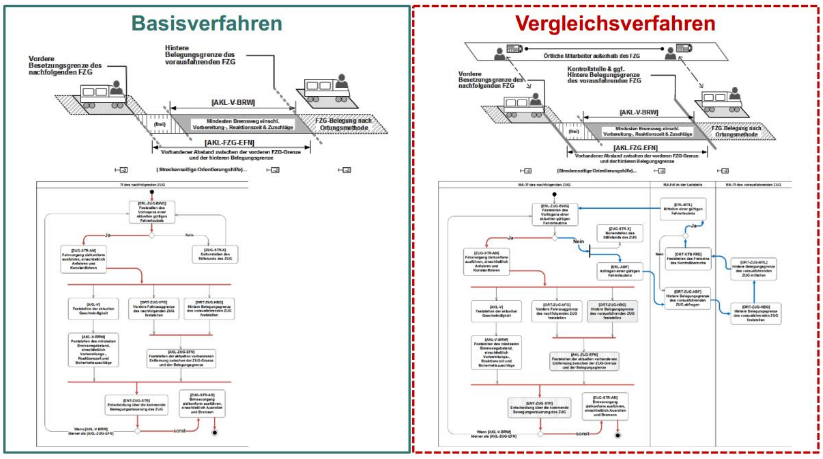

Basisverfahren
Vergleichsverfahren
Vordere Besetzungsgrenze des nachfolgenden FZG
Hintere Belegungsgrenze des vorausfahrenden FZG
Örtliche Mitarbeiter außerhalb des FZG
Kontrollstelle & ggf. Hintere Belegungsgrenze des vorausfahrenden FZG
[AKL-V-BRW]
[AKL-FZG-EFN]
Mindesten Bremsweg einschl. Vorbereitung-, Reaktionszeit & Zuschläge
FZG-Belegung nach Ortungsmethode
Vorhandener Abstand zwischen der vorderen FZG-Grenze und der hinteren Belegungsgrenze

Figure 1. Compare risk of operational methods with generic basic activities (Huang (2016))

We adapted his concept to compare the risk of using different operational modes in an operational method. However, the concept of Huang is not practicable to be used to compare the degraded modes systematically and efficiently. First, the effort to set up the detailed process for all the operational modes including the failure modes is too immense. Secondly, his method concentrates only on comparing the risk of the whole process. However, it does not include a systematic way to compare the partial risks of the different operational modes and it lacks any methodical way to organize all the related degraded modes into a layered structure.

Knowing the disadvantage of Huang’s method, we have realized that in order to compare the operational modes including its degraded modes efficiently and systematically, we first need a mapping framework. This mapping framework should be able to organize the operational modes generically into a process-based but layered structure. It should also enable the allocation of a certain operational mode to the generic requirement which it supposed to be achieved in the generic process.

Using this adapted concept, we have logically and structurally divided our method into two frameworks: the “mapping framework” and the “risk assessment framework”. It is essential to set up the mapping framework as preparatory work for the ongoing risk assessment. The mapping framework is constructed to offer a systematic overview of the alternative paths, which can be used to achieve a certain generic requirement. Using the result of the mapping framework as input, the risk assessment of selected alternative paths can be done in a controlled manner and make our method effective and practical.

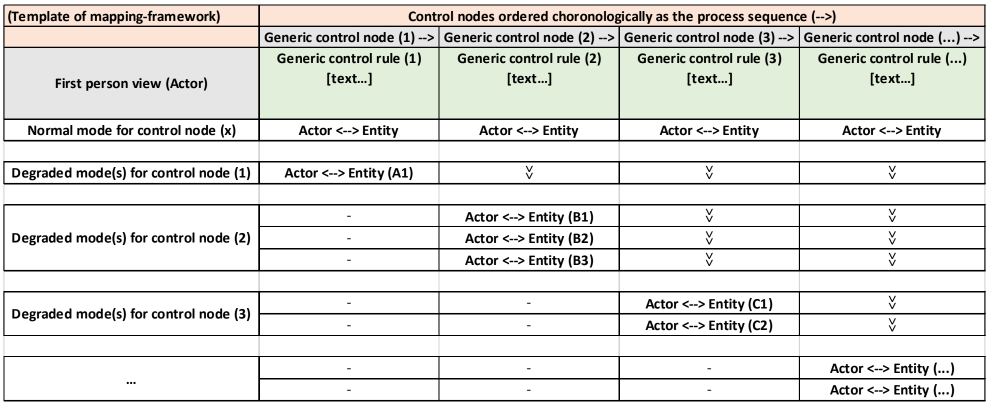
2.3 The human centred mapping framework for layered degraded modes

The structure of this framework, see Figure 2, is particularly developed to fit the systematic of the German rule book for train operators. The operational rules for train operators in Germany are written in an event-based systematic, starting with any event which is a deviation from normal operation. Therefore, existing degraded modes are included almost completely.

But the disadvantage of the event-based systematic is that, the operational rules for normal operation are merely included. To include these rules, the rules would have to be provided in a process-oriented systematic. In order to compare the risks of different degraded modes across a certain process, but without setting up the detailed process, we decided to use generic control nodes to construct a simplified generic process to resemble the process in this framework.

Those control nodes exist usually as safety-related control rules in the event-based operational rules, we name it “rule of control”. They denote the requirements that the degraded mode needs to fulfil as in the normal operation. For example: To ensure that the train is protected by a signal at Danger after entering a block section. Two other types of rules are also needed and can be identified from the rule book and documented for each control node. The first type “rule of alternative” describes the alternative degraded modes which can be used to fulfil the requirements at the control node. For example, as stated in the German rule books (DB (2017)), the train operator can ask the neighbouring train operator, a ground staff on site or a train driver as alternative, to report the completeness of the train and ensure the clearance of a certain section. The second type “rule of transition” describes the default valid transitions of operational modes between two control nodes and will be needed in the risk analysis to estimate the subsequent effect of certain failure. For example, if the train operator cannot clearly identify the last train ahead by clearance check, the next train has to be authorized to pass through the relevant section on sight as default valid action. The mapping framework in figure 2 does not show the rules of alternative and transition. These two kinds of rules will be documented separately, using a similar structure in table-list form during the mapping process.

Every operational mode in the framework, both normal and degraded, is described in an “actor-entity” relationship. The feature of this framework is its first person view, in our case the view of the train operator. It means that the train operator has always the role as “actor” in the relationship, except when the computer takes over the role of train operator, like in the normal operation. The concept of the first person view is also influencing the generic control nodes. That is to say, each requirement at each control node must be able to be accomplished by the first person as actor. The entity which the actor interacts with can be a staff, a technical system, etc. This feature enables an interaction based and human centred risk assessment which is displayed in a process-oriented structure.



(Template of mapping-framework)	Control nodes ordered choronologically as the process sequence (-->)			
	Generic control node (1) -->	Generic control node (2) -->	Generic control node (3) -->	Generic control node (...) -->
First person view (Actor)	Generic control rule (1) [text...]	Generic control rule (2) [text...]	Generic control rule (3) [text...]	Generic control rule (...) [text...]
Normal mode for control node (x)	Actor <--> Entity	Actor <--> Entity	Actor <--> Entity	Actor <--> Entity
Degraded mode(s) for control node (1)	Actor <--> Entity (A1)	︾	︾	︾
Degraded mode(s) for control node (2)	-	Actor <--> Entity (B1)	︾	︾
	-	Actor <--> Entity (B2)	︾	︾
	-	Actor <--> Entity (B3)	︾	︾
Degraded mode(s) for control node (3)	-	-	Actor <--> Entity (C1)	︾
	-	-	Actor <--> Entity (C2)	︾
...	-	-	-	Actor <--> Entity (...)
	-	-	-	Actor <--> Entity (...)

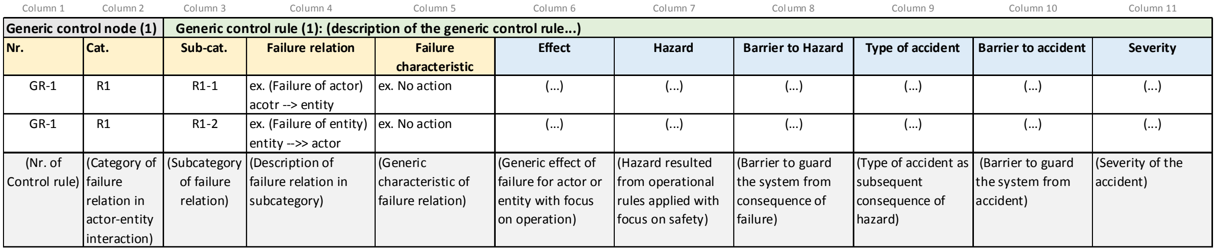
Figure 2. Template of mapping framework

As shown in Figure 2, the generic control nodes at the top of the framework are ordered chronologically from left to right to resemble a simplified process sequence. For each control node, there is at least one normal mode and it can have zero to unspecific number of degraded modes. For example, at the generic control node (2), there exist three degraded modes B1, B2 and B3. All of them have the ability to fulfil the requirements of the control rules independently. The order of the degraded modes B1, B2 and B3 can represent the priority of the degraded mode to be used, but this is not definitely needed.

The choosing of the control nodes is vital for building up the simplified process. We argue that, due to the high reliability of the railway system, normally not all of our systems and not all of the sub-processes will fall into degraded mode at the same time. Therefore, even though the control nodes are connected together logically to resemble a process, the operational modes between control nodes should be independent from each other. For example, if the degraded mode (B2) is used at control node (2), but the normal mode at the control node (3) still works, if the rule of transition permits, the process can go back to the normal mode at the control node (3). By using this concept, we can represent or predict the possible development of the process with combinations of the degraded modes from control node to control node. In the following paragraph, we will show how the result of this framework can be used as structured input for the risk assessment.

2.4 The FMECA oriented risk assessment framework for comparison degraded modes

The structure of the risk assessment framework is aligned with the FMECA (Failure Mode, Effects and Criticality Analysis). As shown in Figure 3, the framework can be divided into two areas. The first area (column 1 to 5) includes the failure relations and failure characteristics, with column 4 taken from the mapping framework. The actor-entity relations from figure 2 are further detailed into the relations: failure of actor and failure of entity. In combination with the generic characteristic (ex. wrong time: no action, too early, too late) of the failure relation, all failure modes to be considered can be set up. The second area (column 6 to 11) includes a structure for analyzing the consequence of the failure modes.



Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9	Column 10	Column 11
Generic control node (1)		Generic control rule (1): (description of the generic control rule...)								
Nr.	Cat.	Sub-cat.	Failure relation	Failure characteristic	Effect	Hazard	Barrier to Hazard	Type of accident	Barrier to accident	Severity
GR-1	R1	R1-1	ex. (Failure of actor) acotr --> entity	ex. No action	(...)	(...)	(...)	(...)	(...)	(...)
GR-1	R1	R1-2	ex. (Failure of entity) entity -->> actor	ex. No action	(...)	(...)	(...)	(...)	(...)	(...)
(Nr. of Control rule)	(Category of failure relation in actor-entity interaction)	(Subcategory of failure relation)	(Description of failure relation in subcategory)	(Generic characteristic of failure relation)	(Generic effect of failure for actor or entity with focus on operation)	(Hazard resulted from operational rules applied with focus on safety)	(Barrier to guard the system from consequence of failure)	(Type of accident as subsequent consequence of hazard)	(Barrier to guard the system from accident)	(Severity of the accident)

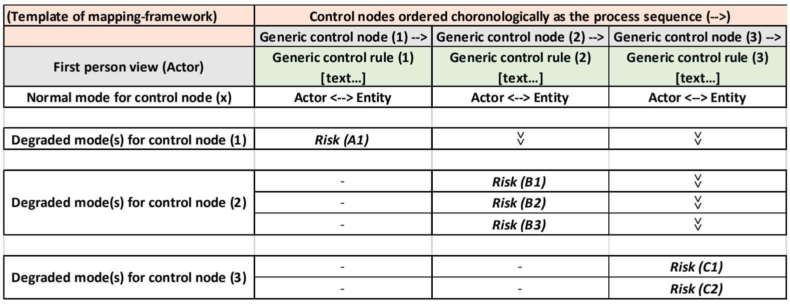
Figure 3. Template of risk assessment framework

The analysis begins with considering the generic effect of the failure mode for actor or entity on operations, followed by analyzing the hazard resulting from the failure mode and the applied operational rules with a focus on safety. Type of accident as subsequent consequence of hazard and the severity of accident will also be considered. The other feature of this framework is that we incorporated the barrier model. In our barrier process model, we consider two kinds of barriers: barriers to prevent the hazard to occur; barriers to prevent the accident to occur. The barrier acts as reduction factor in the risk assessment. Logically, we can express the barrier process model as follows:

failure → [barrier to prevent hazard] → hazard → [barrier to prevent accident] → accident

However, in our framework, we place the barriers rationally in reverse order. The barriers are ordered behind hazard and accident respectively. The advantage of this order is that it helps the user to focus first on the consequence (usually worst or worst credible case) of a failure mode and afterwards to concentrate on identifying the (additional) barriers which are not necessarily documented in the operational rules.

Due to the risk oriented structure of the framework, it is possible to evaluate and summarize the result with known methods like Risk Priority Number (RPN), Best Practice Risk (BP-Risk). The analyzed risk can then be added to the mapping framework to have a systematic overview of the risk of using different degraded modes across the process, see Figure 4. However, the discussion about the evaluation and of different operational methods is not in the scope of this paper.



(Template of mapping-framework)	Control nodes ordered choronologically as the process sequence (-->)		
	Generic control node (1) -->	Generic control node (2) -->	Generic control node (3) -->
First person view (Actor)	Generic control rule (1) [text...]	Generic control rule (2) [text...]	Generic control rule (3) [text...]
Normal mode for control node (x)	Actor <--> Entity	Actor <--> Entity	Actor <--> Entity
Degraded mode(s) for control node (1)	*Risk (A1)*	︾	︾
Degraded mode(s) for control node (2)	-	*Risk (B1)*	︾
	-	*Risk (B2)*	︾
	-	*Risk (B3)*	︾
Degraded mode(s) for control node (3)	-	-	*Risk (C1)*
	-	-	*Risk (C2)*

Figure 4. Summary of the risk using different degraded modes at certain control node

3. Example “Räumungsprüfung (Clearance check)”

3.1 A brief introduction to German method for clearance check in degraded operation

On German automatic block lines, the stop aspect on automatic block signals is absolute, i.e., it does not differ from the stop aspect on interlocking signals. A train must not pass any signal in stop position without authority from the operator. In case of a block system failure, the train operator has to perform a clearance check for the relevant block section (see Figure 5 for illustration).

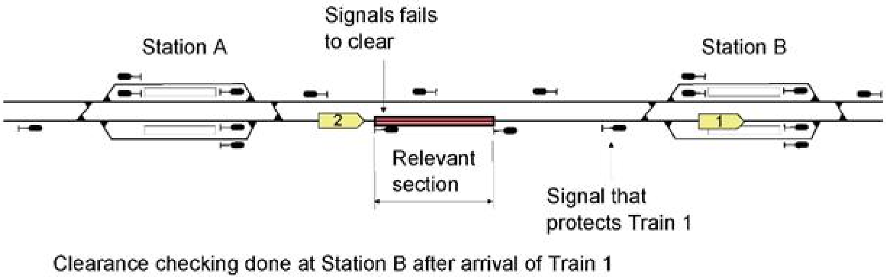

Signals fails to clear
Station A
Station B
2
1
Relevant section
Signal that protects Train 1
Clearance checking done at Station B after arrival of Train 1

Figure 5. German method for train operation in degraded mode (Pachl (2017))

This clearance check is commonly required in these two cases:

- Case 1: A train is to be authorized to pass a signal in stop position that controls the entrance of a block section. That signal can be either an automatic block signal or an interlocking signal.
- Case 2: A block section that has remained occupied or locked after the passage of a train has to be reset by the operator. Since, in such a case, the signal governing entrance to that section may clear even if it is not safe to proceed, safety has to be ensured under staff responsibility.

If in case 1, the train operator cannot clearly identify the last train ahead or the completeness of the last train ahead cannot be confirmed, the next train has to be authorized to pass through the relevant section on sight. The train operator is required to perform a clearance check for the next train. Without having confirmation of the completeness of the last train ahead, the operator cannot be sure whether a track occupation shown on the user interface is caused by lost equipment obstructing the track, or by other reasons.

If in case 2, the train operator is going to reset a block section under staff responsibility, the next train has to be authorized to proceed on sight. The order to proceed on sight must be issued before the resetting command is executed. If the resetting fails, the operator has to secure the signal protecting the relevant section in stop position. Then, the operator is required to perform clearance checks for all following trains until a signal maintainer has re-established normal working of the block system. (Chapter adapted from Pachl (2017)).

For a clearance check of a block section, the train operator has at first to identify, which train was the last train ahead that passed through the relevant block section. For that train, the following three criteria have to be confirmed:

- Criteria 1: The train has arrived at a designated section beyond the relevant block section, where the clearance check can done.
- Criteria 2: The train must be protected by a signal at Danger. This includes the clearance of the overlap beyond that signal.
- Criteria 3: The train must be complete.

3.2 Identifying control nodes and selecting failure characteristics

As stated in the previous paragraphs, our frameworks can be used to access the risk at one control node, as well as to access the risk across all the control nodes in process view. To getting started with understanding the framework, we focused the scope of analysis in this paper to access the risk of human errors at one single control node. The following conditions have been set for the scenario “A train has been stopped due to a signal at “Danger” before a section in a line with automatic block system”. The train operator in the operational control centre realized that a train stopped and tries to give the train authority to proceed. The cause of why the signal did not show “Clear” automatically is undefined; it can be a failure or can also be a normal occupation of the section ahead without any failure. Resetting block is not considered. The process in this scenario begins with the train operator trying to identify the last train, followed by the clearance check for that train and the giving of authority for the train to proceed. It ends with another clearance check after the train has arrived at the designed station.

We begin the analysis with identifying the control node from the operational rules. The characteristic of a control node is that requirements to be fulfilled at each control node shall be done only within a single actor-entity relation. For example, in criteria 2 of the clearance check that described in Chapter 3.1, the activity "train must be protected by a signal at Danger" and the "clearance of the overlap beyond that signal" can be identified as two different actor-entity relations in our framework. They are "operator←→user display (signal)" and "operator←→user display (track section)". Therefore, they should be assigned into two different control nodes. Sometimes, several criterions can be fulfilled by one actor-entity relation in one degraded mode. For example, as stated in the German rule books (DB (2017)), to report the completeness of the train and ensure the clearance of the relevant section including overlap, the train operator can use the safety verified user display, he can ask the train driver who has already left the designed section, the neighbouring train operator or a ground staff on site, respectively. In this case, two criteria of clearance check, the completeness of the train and the clearance of the relevant section including overlap, can be fulfilled by one actor-entity concurrently. Rationally, these two criteria can be allocated to the same control node from the view of actor-entity relation. But not necessarily, if we consider the separation of section and overlap in German interlocking logic, it can be sometimes useful to keep it apart in the analysis. However, we consider them first as one control node here and use it for the following analysis. The control rule at this control node can be generically described as "Can the clearance of the relevant sections including the overlap be ensured after the train has arrived the designated station?"

From the German rule books, we can identify at least four alternatives for this control rule, more specifically four degraded modes in form of actor-entity relation. They are operator ←→user display (track section), operator←→train driver, operator←→ground staff on site and operator←→neighbouring operator. The relation with train driver, ground staff and neighbouring operator can be further summarized into "operator←→staff" relation for generic analysis. To enable a human centred risk assessment, we further divide each relation into "failure of actor" and "failure of entity" respectively. Subsequently, we select three failure relations which related to human error (failure of operator with tech., with staff and failure of staff) in combination with selected failure characteristics to set up the human related failure modes for the risk assessment. Based on our actor-entity model, we defined that when a [defined actor] does a [defined action] to a [defined entity] at a [defined point of time], then an interaction can be considered as correct from the viewpoint of system process. For our example, we looked at the train operator as actor and considered only single failures in the interaction. Under this presumption, we can derive four generic failure characteristics which are resulting in five types of single failure as shown in Table 1.

Table 1. Single failure and failure characteristics considered in the example

failure characteristic used in FMECA, actor did ...	Action of actor from system process view	time of the action happened from system process view	Entity which the actor interacted with from system process view	Action of actor from actor's view afterwards
1-nothing	no action	point of time	-	forget
2-too early	defined action	too early	defined entity	thought it was right
3-too late	defined action	too late	defined entity	thought it was right
4-wrong	defined action	point of time	wrong entity	thought it was right
	wrong action	point of time	defined entity	thought it was right

3.3 Accessing risk of human errors

The combination of the selected three failure relations and the four failure characteristics, we get a total of 12 human related failure modes to be analyzed. The identified "rule of transition" will then be needed to predict the consequences of the failure modes. As the evaluation method is not in the scope of this paper, we use the probable severity of the resulting accidents to discuss the results of the assessment. Based on the possible speed at the moment of collision, we divided the severity of accident into four levels, from 1-minor to 4-disastrous. Later, we will probably use a more refined set of accidents, e.g. taken from 0831-103 (DIN (2014)).

Table 2. Result of human centred risk assessment

Summary: Number of the accidents from totally 12 human errors in CR-2, arranged by failure characteristic					
Severity of accident	accident	No action	Too early	Too late	Wrong action
4-disastrous	Collision with train ahead under speed (Vmax)	0	0	0	0
3-crucial	Collision with train ahead under speed (40+)	1	1	0	3
2-marginal	Collision with train ahead under speed (on sight)	2	0	0	0
1-minor	None / negligible	0	2	3	0

As shown in Table 2, five of the twelve failure modes can cause crucial severity by accident, two of the failure modes can result in marginal severity. However, the severity level marginal is the result of standard process to proceed on sight. The potential risk of proceeding on sight under staff responsibility is generally accepted in today's railway operation and will not be discussed further here. We concentrate on the five failure modes with crucial severity. Three of them are resulting from the failure of the operator while giving the train the authority to proceed with special order like auxiliary signal. The failure modes are that the operator:

- … (no action) forgot to check the clearance with using user display or
- … (wrong) checked the clearance flawed with using user display or
- … (wrong) did the communication flawed with staff

The other two failure modes are resulting from the failure of the staff in that the staff:

- (wrong) gave the wrong info about the clearance… or
- (too early) gave the info about clearance of track too early…

Based on this erroneous action, the operator gave the train the authority to proceed. Moreover, in this analysis, we could not find any direct barrier which can guard the system from hazard or accident after the human error occurred. The attention of staff is the only indirect barrier which can be found to prevent the crucial consequence which might result from human error.

4. Discussion

4.1 Effect of multiple failures and other failure characteristics

The selection of failure combinations and characteristics is critical for reasoning the scope and the completeness of the risk assessment. Since we only considered the single failure in our example, we thus need to ask inevitably how the multiple failures can affect the existing result of the analysis. We have done a simplified preliminary analysis and found that multiple failures will generally cause the same hazard in our example this is that the train (or wrong train) enters an occupied section with special order from the train operator. Nevertheless, the type of accident and the severity of the accident may differ from the single failure. Secondly, there exist indeed a number of other characteristics of human errors in the literatures like wrong duration, wrong intensity, etc. (Hammerl (2011)). Ideally, a risk assessment should cover all aspect of the failures. Therefore, we will focus part of our research on identifying a method to cover all human failure modes in a systematic way. For reasoning the scope and the completeness, the effect of multiple failures and other failure characteristics will need to be further analyzed with using selected risk evaluation method.

4.2 Effect of IT security attack on the scope of risk assessment

We've discussed the different failure characteristics and the multiple failures in the previous paragraph. However, all the failures we talked about resulted from action done with good intention of the actor. The difference of an IT security attack is that failures are triggered from the attacker intentionally. Certainly, consequences of some IT security attacks are already covered by the existing risk analysis. This is also our main argument to first adapt the operational rules in degraded mode to make it safer. The critical issue of IT security attack is the content of the "wrong action" in combination with the "failure characteristics" which have been triggered intentionally. The question is: can our system do some "wrong action" resulted from IT security attack which we do not know? Moreover, how far the consequences of IT security attacks can be handled by today's degraded modes and to what extent the degraded mode and operational rules need to be adapted due to threat of IT security attack? Those questions can be further analyzed with our frameworks in that we extend the failure characteristics to include the catalogue of typical attack scenarios as given in 0831-102 (DIN (2013)) to analyze which human failure relations in the degraded mode are more vulnerable.

5. Conclusion

In this paper, we've introduced two frameworks which can be used to construct a layered structure for degraded modes and compare the risk of using different degraded modes accordingly. We've demonstrated that with using this framework, we can enable a human centred risk assessment for operational modes and can identify the failure modes with crucial consequence in a very structured and systematic way. The effect of multiple failures in the interaction, diverse failure characteristics and IT security attacks need to be further considered and can be systematically analyzed with using the introduced risk assessment framework. Moreover, based on the risk oriented structure of the framework, the risk of using different degrade modes at a single control node or across the whole process can be summarized and compared with known risk evaluation methods. The discussion of using different risk evaluation method is not in scope of this paper and will be further analyzed in our ongoing research project SysRULES (2017-2019) which granted from the Karl-Vossloh-Stiftung in Germany.

References

Bainbridge, L. (1983). Ironies of Automation. Automatica, Vol. 19, No. 6, 775-779.

DB Netz AG (2017). Fahrdienstvorschrift – Richtlinie 408.

DIN VDE V 0831-102 (2013). Electric signalling systems for railways - Part 102: Protection profile for technical functions in railway signalling.

DIN VDE V 0831-103 (2014). Electric signalling systems for railways - Part 103: Identification of safety requirements for technical functions in railway signaling.

Hammerl, M. (2011). Analyse der menschlichen Einflussfaktoren und Zuverlässigkeit im Eisenbahnverkehr. Technische Universität Carolo-Wilhelmina zu Braunschweig.

Huang, P.C. (2016). Risikobasiertes Verfahren zur Bewertung von eisenbahnbetrieblichen Rückfallebenen – erste Ansätze. Presentation on the 9th Workshop "Safety in Transportation (SiT)" on 14. and 15. November 2016 in Braunschweig.

Pachl, J. (2004). Vorschlag für eine neue Systematik der Betriebsverfahren deutscher Eisenbahnen. Der Eisenbahningenieur, 7, 5-10.

Pachl, J. (2017). Block and Interlocking Principles. Lecture notes.