Generic Hazard List for Railway Systems

Martin Pope\(^1\), Jörn Drewes\(^2\), Jörg May\(^2\)

\(^1\)UIC Euro-Interlocking Project, Zurich, Switzerland, \(^2\)Institute for Traffic Safety and Automation Engineering, Technical University of Brunswick, Braunschweig, Germany

Abstract

Safety requirements for railway systems must be developed in consideration of the potential hazards, which are usually defined by group experts in hazard lists at HAZOP (Hazard and Operability Studies) meetings. While a broken chassis screw and a derailment can both be considered as hazards the abstraction layers are completely different. This means that the definition process for a hazard list requires a consistent system view and a structured approach. This paper provides a guideline to a generic hazard list with a new definition method for railway systems. Each determined hazard is transformed into its converse thus providing a set of high-level safety relevant requirements for railway signalling. These requirements can be used to match existing functional requirements in mitigation, or additionally to formulate new requirements where vacancies are discovered.

Introduction

The foundation of the Euro-Interlocking Project (EIP) is the ongoing capture process for signalling principles and associated functional requirements for interlocking systems across the European railways. The resulting analysis and reduction towards commonality using CENELEC norms to establish the processes has resulted in a highly structured approach to this work. The early phase CENELEC norms represent only the work above the notional horizontal line between client and supplier responsibilities in the \(V\) lifecycle. The work done here is also representative of this area, “the requirements definition phase” CENELEC [1] also requires in its “Phase 3”, a hazard identification process to be established for the system to be delivered.

This paper sets out to describe in some detail the latest work done in the field of Generic Hazard List (GHL) development, and the relationship of that work to the EIP. The Technical University of Braunschweig together with a group of railway signalling and functional requirements engineers have been utilizing the requirements of the CENELEC norms to develop a cost cutting approach to the interlocking development process by identifying the commonalities between railway signalling requirements in Europe. From this process a generic kernel of interlocking functionality supported by generic processes for hazard identification, verification and validation is being developed with the eventual goal of harmonization of principles, both signalling and operating, across Europe supported by unequivocal data and generic processes.

1. Hazard Identification Process

Traditionally, hazard identification has been performed by experts by virtue of their experience with accident analysis and the resulting findings. In addition to this, the experts’ system knowledge helps in a way to predict possible hazardous situations as experts often unknowingly perform risk analyses by tracing the theoretical chain of cause and effect during the identification process and deciding to either follow or to disregard the individual hazard. Obvious hazards are then mitigated by either changing the system or by defining functional requirements while unobvious hazards are disregarded. The problem of this procedure arises from two sides. On the one hand the experts tend to focus on technical failures at too detailed a level that actually do not exist during the design phase until an implementation is framed. On the other hazards may accidentally not be considered to be possible due to insufficient estimation of probability during the identification process.

The solution for theses problems is to remain on a constant level of detail during the hazard identification process and to avoid any estimation about the probability of an identified hazard. The probability of a
hazard shall be solely determined during the risk analysis process. The purpose of the hazard identification process is to be focused on the identification of any possible hazard regardless of probability estimations. Both solutions can be achieved by a structured and methodology based hazard identification process that will be shown in the following text.

1.1 Hazard Definition

In order to identify a hazard the content needs to be defined. Under consideration of the European CENELEC norms[1], the hazard is defined to be “a physical situation with the potential of human injury”. This expression describes a state from which it is likely that damage will be suffered due to, for example, an accident. The condition-event-net in Figure 1 shows the causal dependencies between damage (human injury), the potential of damage (hazardous state) and the causes leading to this situation [7, 8]. In this case the hazardous state expresses the physical situation with the potential of human injury following the transition “accident occurrence” still remaining a possibility to reach the safe state following for example a protection process or just pure luck. Both transitions can be attributed stochastically resulting in rates. In order to describe the hazardous state adequately for future functional requirements and risk analysis it was helpful to include the hazardous conditions (causes) and the undesired events (possible accident [5, 6, 9]) into the hazard definitions (refer to the dotted line in figure 1). This enables structured estimations concerning the severity of damage for risk analysis and supports the functional requirements development process in order to mitigate against identified hazards.

![Causal dependency analysis for a solid hazard definition](image)

Responsible for system hazards are hazardous conditions that can be linked to the system structure on one hand and to the system functionality on the other. As only hazards provoked from the considered system are relevant in terms of system safety requirements, external influences to the systems as terrorism or manipulation will be disregarded.

1.2 System Structure Analysis

Analysis of the system structure implies knowledge about the system and especially about the system boundaries. Within the EIP context the system boundary is defined to be the interlocking system kernel and in particular the interlocking logical system. Although the adjacent physical elements like points, signals etc. are considered in order to define clear relationships between the driven elements and the logic, the causes of hazardous conditions are not identified inside the peripherals. While both the incorrect driving command from an interlocking logic to a point and the incorrect point movement (i.e. due
to point machine failure) invoke a possible hazardous state the incorrect driving command is the responsibility of the interlocking system whereas the point itself is responsible for the incorrect point movement.

Corresponding to the domain knowledge documents prepared in the framework of the EIP, the system structure presented in Figure 2 follows the allocation of functional requirements to the physical elements. This only describes the functional arrangement inside the interlocking logic [3]. It does not imply any particular functional or software architecture from an implementation standpoint.

![Figure 2 Static Structures of Logical and Physical Elements for Interlocking Systems](image)

Every static element described in this figure will execute different functions. In a next step this functionality will be analyzed and linked to both physical and logical elements.

### 1.3 System Functional Analysis

The functional structure for interlocking systems is described using execution processes and communication values. While the execution processes show the actual function of the resource, which can either be a physical or a logical element (ref. to figure 3 - physical or logical process) the communication between the physical and logical resources is distinguished between detected values as for example sensor information and driving values (i.e. command telegrams). Physical processes are executed by the physical elements (i.e. point movement execution) while Interlocking Logical (IL logic) processes execute according to requirements derived from signalling principle (i.e. making decisions according to defined rules). Since the focus of the hazard identification in this project relates to the interlocking system communications between logical and physical elements as well as between different logical elements, communications between different physical elements have been disregarded.

According to the system structure in figure 2 the functional analysis is performed for all logical elements shown inside the interlocking kernel as well as for the physical elements having direct relationships to these. Figure 3 only shows the general approach to the process of describing the functionally of the
interlocking. Concentrating on a single element will show the cyclic dependency of detected value, logical process, driving value and physical process (ref. figure 4) in analogy to a basic control loop with a comparison between set-values (input by rules, objectives etc.) and the actual system information expressed by detected values. In case of varying values the logical process (i.e. decision making or control tasks) generates driving values that are executed by the physical processes or in case of internal communication, by another logical process. The execution of the driving values leads to changing system information and therefore to changing detected values until set-value and detected value match. This cyclic procedure expresses four parts of functionality for each resource. After analysis of the structure and of the functionality of the interlocking system possible hazards must be identified.

Figure 3 System Functional Structures for Interlocking Systems

Figure 4 Control loop structures as a basis for functional analysis

1.4 Deriving Textual System Hazards from Hazards Tables

The bases of the hazard identification process demonstrated in this approach are the hazard tables. These combine the resources from the structural analysis with the four functional parts (detected values,
logical process, driving values and physical process) of the functional analysis. Figure 5 shows an example for a point-to-point logical relationship.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Functionality</th>
<th>accident characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>detected values</td>
<td>logical process</td>
</tr>
<tr>
<td></td>
<td>detected direction values of a point (left/ right)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>detected/failure values of a point (trailing/ not trailing)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>direction control of a point (left/ right)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>status control of a point (supervision)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>direction steering values to a point (move left/ move right)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>direction change of a point</td>
<td></td>
</tr>
<tr>
<td>Point (Pt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F-Pt-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F-Pt-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F-Pt-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F-Pt-4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F-Pt-5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F-Pt-6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5 Hazard Table as an instrument for structured hazard identification

On the left hand side the resource is shown (extracted from the system structure). The top row presents the functional part as described in the previous section. The functionality is separated into the four basic parts (detected values, logical process, driving values, physical process) and according to the functionality of the point the corresponding functions are filled in.

The right side of the table includes accident characteristics that are classified as follows:

- **A1** collision of a railway vehicle with another railway vehicle
- **A2** collision of a railway vehicle with object other than railway vehicle on track
- **A3** collision of a railway vehicle with object other than railway vehicle on level crossing
- **A4** derailment of a railway vehicle on a moveable
- **A5** fire accident of a railway vehicle
- **A6** nature accident of a railway vehicle (e.g. flood, avalanches, etc.)
- **A7** chemical accident of a railway vehicle (e.g. acid)
- **A8** biological accident of railway vehicle (e.g.
A5 derailment of a railway vehicle on a fixed track element
A10 electrical accident of a railway vehicle (e.g. falling catenary)

Each textual hazard is given a unique hazard identification including the resource name (here: Pt for point) the failure-identification (here “3” from F-Pt-3) and the accident characteristics’ id (here “1” from 3-1) as well as a suffix (“haz” for hazard) for superior documents. The combination of this hazard leads to a hazard id: “Pt-3-1-haz”.

The hazard identification process is based on the assumption of either a functional failure or the non-existence of a particular function. This assumption is represented in the table with the diagonal marks inside the cells in the body of the table. For example “F-Pt-3” assumes failing or missing direction control functionality for point logic. Every failure assumption is described with a more detailed example in the original documents. Here for example the explanation is:

“incorrectly applied rule inside the interlocking logic allows the driving of a point into wrong directions. A point providing flank protection may be driven into a wrong position. As a result a collision may occur”.

For every specific accident classification that is possible for a functional failure a crossed cell in the corresponding column and row will exist with an identifier. Here one example is “3-1” and the textual hazard is then derived by using pre-defined sentence structures including the possibility of an accident (A1 – A10) due to a failure description (F-Pt-#). For the example shown the textual hazard is as follows:

“Possible collision of a railway vehicle with another railway vehicle due to incorrect direction control of a point” (Pt-3-1-haz)

2. Functional requirements for interlocking systems

EIP functional requirements are the compiled input from many hours of interviews with railways by a small team of signalling engineers based in Zürich, Switzerland. The need for the project has been driven by the high cost of interlocking systems caused by the differences between railways and their individual requirements and the belief that this could be dramatically reduced if the generic part of the logical construct could be distilled, and applied to each railway. Only by capturing all the requirements can the true extent of these differences be ascertained and a process begun whereby railways can examine their needs from a functional standpoint rather than a historical one, and work towards a harmonised functional environment. This process, if successfully achieved can lower the cost of interlocking systems considerably, and open the market to competition; possibly from suppliers previously unknown to the industry. Imagine a “Nokia” Interlocking system in the future.

With the ongoing drive in both Europe and other countries towards communication based signalling systems e.g. ERTMS - ETCS / ATCS, the processes already established in this traditional interlocking project can readily be expanded to the communications based environment and the architectures envisaged within it.

2.1 High Level Safety Relevant Requirements

While general operational & functional requirements enable (efficient) system operation the safety relevant functional requirements ensure that the operation of the system does not permit any unwanted hazards. After identifying the extent of system hazards in the first section of his paper, each of those hazards must be transferred into safety relevant requirements. Since the level of detail in each hazard
does not allow consideration of any implementation issues, the safety relevant requirements can only be derived as high level requirements without any implementation approach.

The hazards identified inside the hazard tables have been formulated using structured sentence syntax, which will be used to automatically generate safety relevant functional requirements. By negating the cause and inverting the sentence blocks while adding typical filler words in order to formulate a well-formed sentence, all hazards may be transformed into requirements.

"Possible collision of a railway vehicle with another railway vehicle due to incorrect direction control of a point" (Pt-3-1-haz)

"The interlocking system shall ensure that the direction control of a point does not enable a collision of a railway vehicle with another railway vehicle" (Pt-3-1-HLreq)

Each high-level safety relevant requirement is labelled with a unique identifier so the linking and traceability to the original hazard persists.

2.2 Cross referencing between requirements

The requirement engineering process ensures that the processes employed between idea and reality are clearly defined, and provides a traceable path through that process. At any or every stage of the process, requirements definition and subsequent derivation by the manufacturer enables a verifier, usually an ISA or Notified Body (NOBO) to ensure that quality and safety rules have been adhered to. This control of the process can therefore lead to shorter validation times at the commissioning phases of a product system or subsystem by ensuring that the design principles have been matched to the requirements so ensuring that the safety of the product can be more readily established.

Whilst the CENELEC norms have been used in the industry for some number of years now, the concept of, and indeed the ability to, cross reference requirements between safety, form, fit, function and the "rules" is however a relatively new idea. It has been the brainchild of the EIP team in Zürich, together with its sub-contracted experts since 1998, and its ideals are well established in Europe, with its qualitative requirement suite having been used in tendering for new interlocking equipment by some railways. The team have focussed during the last two and a half years with the railways of Europe to derive the interlocking kernel functions associated with their signalling principles and rulebooks. This work, compiled and maintained in the DOORS environment is central to the requirements capturing process, and the environment permits the linking of elements by relationship or commonality of function.

The document [1] outlines this process in the so-called "V" lifecycle for a product or system that controls its existence from concept to de-commissioning. This process has been heavily adopted among the European railways and other industries as latterly it has become one of the accepted methods by which transportation safety systems and subsystems such as interlocking may obtain certification for service.

This paper deals specifically with the interlocking safety kernel and the manner in which the phase 3 and 4 processes from [1] have been applied in the EIP. These two phases of the system development process relate to the sequences to be followed before any design work or functional derivation is performed. Failure to follow these steps has in the past led to some notable delays in certification, and expensive reworks to designs that are not sufficiently proven for function and/or safety. To this end, the country specific safety requirements for interlocking systems are also integrated into the EIP database (where available), and these enable us to prove that each of these is mitigated against by the inclusion of one or more functional requirements.
The EIP has taken the hazard identification process down the path shown above as developed for the identification of functional requirements. Each logical function or element in the hazard identification process has been assigned the same terms and structure as seen in Figure 6, allowing a greatly simplified tagging and linking process between the products of the two phases outlined in [1].

To satisfy the Phase 3 requirements [1], there must be a hazard identification process undertaken which was already presented in section 1 above. The establishment of a link between the Generic Hazard List (GHL) the interlocking functional requirements has led to further work where the interlocking functional requirements have been tagged in the database as either “safety” requirements or purely functional, and the individual functional requirements have been cross referenced against the derived hazards inside the GHL.

The selected supplier according to the CENELEC process develops technical or “derived requirements”. The process for this derivation from the client supplied functional baseline sits under the Client / Supplier line in the “V” lifecycle, and their processes are therefore not represented here.

3. **Technical application for requirements analysis in combination with identified hazards**

EIP functional requirements gathered from railway signalling experts across Europe and indeed around the world have been stored in the DOORS Database environment.
Within the DOORS™ environment, the ability exists to link functions across module boundaries, and to retain a full change history. The GHL and the functional requirements are installed, and from the original exercise, each requirement is being linked to a high level requirement derived from the converse of an identified hazard. Each high level requirement is linked as well directly to its originating hazard. As an additional process, test procedures are being written and installed in DOORS™ to verify the correctness of the functional requirements against either a formal model constructed in UML or similar, or in fact an existing or test interlocking. This process does not ensure the completeness of the requirements, but does allow one to evaluate the degree to which their text is unequivocal; an extremely desirable element in the writing of functional or other requirements.

Figure 7 below shows the theoretical linking between the “Power Point” functional module [4] and the “Hazard List” phase 3 module in a DOORS™ snapshot. In reality this is performed using virtual links between objects in the database that cannot be lost over the course of history. The ability of DOORS™ to filter requirements specifically for each railway, and the power of DXL scripts in the DOORS™ environment to enable the derivation of the “common core” between railways allows us to see quite clearly those requirements tagged as safety or purely as functional, to be cross checked against the hazard list to ensure that all relevant hazards have been linked.

The completion of this linking exercise will ensure that a complete functional kernel is linked directly to each of the derived hazards and thus closes the circle for pre-implementation recommended within the CENELEC norms [1]. Completion of the process allows a fully functional set of requirements to be used in a tendering process, and provides, at the top right hand side of the “V” lifecycle model, the components for a tool to permit verifiable testing and commissioning of the required system. The process also provides a completely traceable path through the process in order to control the management of design changes during the process, and their impact on the derived requirements and the testing processes required for final verification and validation and system acceptance.

4. Summaries and Outlook

The methodology presented in this paper shows for the first time a structured and integrated approach for identifying hazards from the system structure and functionality analysis allowing hazard identifications on
a consistent abstraction layer. By using semi-formal hazard tables the system structure and functionality analysis can be separated from the hazard identification process. The estimation of possible accidents for different system parts can be done by different expert from different domain while remaining the abstraction layer without drifting too much into detail. This also offers the opportunity to run the hazard identification process with distributed structures.

The use of Excel spreadsheets also gives the chance for a highly automated hazard identification process by deriving the resources and the functions from, for instance, UML models. The formulation of hazards and high level safety relevant requirements using structured sentence syntax also allows further automation in cross referencing etc.

Whatever the outcome of design strategies against operating rules etc, the future development of train control systems can be readily engineered using the processes outlined in this paper.

Acknowledgements
We would like to thank the UIC for their commitment to the work, and for permission to deliver this paper to a wider international audience

References