5

Framework for Automation of Hazard Log Management on Large Critical Projects

Lorenzo Vinerbi[1] and Arun Babu Puthuparambil[2]

[1]Resiltech s.r.l., Pontedera (PI), Italy
[2]Robert Bosch Center for Cyber Physical Systems, Indian Institute of Science, Bangalore, India

5.1 Introduction

A hazard (HZ) is any situation that could cause harm to the system or lives. HZ depends on the system and its environment, and the probability of the HZ to cause harm is known as risk. HZs are analyzed by identifying their causes and the possible negative consequences that might ensue. For example, the dangerous failure of a traffic signal could be caused by a logic error in the traffic signaling controller's software program. The consequence could be conflicting traffic flows simultaneously receiving green signals.

A hazard log (HL) is a database of all risk management activities in a project. Maintaining its correctness and consistency on large safety/mission critical projects involving multiple vendors, suppliers, and partners is critical and challenging. IBM DOORS [1, 2] is one of the popular tool used for HZ management in mission critical applications. However, not all stake-holders are familiar with it. Also, it may not always feasible for all stake-holders to provide correct, well structured, and consistent HZ data. IBM DOORS have been reported to be useful in managing DO-178 compliance for avionics [3]. Also, HL in DOORS allows capabilities for tracing requirements and test results. However, DOORS has steeper learning curve and is difficult to use by common people and beginners [4]. Also, they lack validation capabilities [5]. Custom checks may require difficult to use plug-ins which are not generic. This complexity makes it difficult to maintain the rules; preventing reuse in other projects.

This chapter demonstrates a modular and extensible way to specify rules for checks locally at the stake-holder side, as well as while combining data from various parties to form the HL. The HZ-LOG automatization tool simplifies the process of HZ data collection on large projects to form the HL, while ensuring data consistency and correctness. The data provided by all parties are collected using a template containing scripts. The scripts check for mistakes/errors based on internal standards of company in charge of the HZ management. The collected data is then subjected to merging in DOORS, which also contain scripts to check and import data to form the HL.

The requirements of HL tool are:

(i) Perform checks of incoming data from vendors and partners;
(ii) It shall allow to collect and keep log for all information related to identified HZs (and related identified mitigations), structuring information accordingly;
(iii) It shall be possible to manage the status of the HZs and related mitigations, allowing for the control of risk. Only allowed HZ status transitions shall be possible and logging of the related status transition activity shall be kept in the tool for traceability purposes;
(iv) Only RAMS specialist are allowed to manage HZs being necessary no different user profiles for the management of HZs in the tool;
(v) A function of the tool shall allow to extract the "current" status of the project system HL by allowing the creation of documentary reports containing the set of necessary information about the predicted HZs, mitigations identified, and the status of all related risk control activities.

5.1.1 Brief Introduction on DOORS

IBM Rational DOORS is an enterprise-wide requirements management tool, designed to link and manage diverse textual and graphical information to ensure a project's compliance to specified requirements and standards. It represents a layer to perform:

(i) Import documentation into a DB in order to convert free text into requirements;
(ii) Maintain such requirements during the time;
(iii) Relate requirements belonging to different documents (or level of detail);
(iv) Relate requirements to other artefact (e.g., test specification or report).

Due to its features, it is widely adopted in different domain as reference tool to manage requirements and HL.

5.2 Approach

All the activities described in the previous sections lead to a set of HZs and mitigations; which in the end allow to guarantee the safety all along the lifecycle (see Figure 5.1).

The mitigations identified in PHA [6] and SHA [7] shall be evaluated, along with design changes, on a continuing basis, to ensure that risk associated to HZs has been eliminated or lowered to an acceptable or practicable level. The result of this activity shall be stored in the Hazard Log Tool. Some other activities may provide results to be logged, e.g. design implementation schemes, design analyses, test specifications and test reports etc. Whilst main HZ analyses are planned by the project's safety plan, [7] other safety analyses and project activities providing results to be logged in the HL have no plan. It is the Safety Organization's responsibility to log the outcome of safety activities when resulting new HZs as well as to record all the information necessary to provide final evidence of safety.

A template with configuration and script is created and sent to all participants in the project. Template fields are listed and explained in Table 5.1. Table 5.2 reports possible configurations for mapping DOORS fields into excel ones, while Table 5.3 is an example of configuration for excel template that specifies allowed combination of hazard frequency, severity, and risk

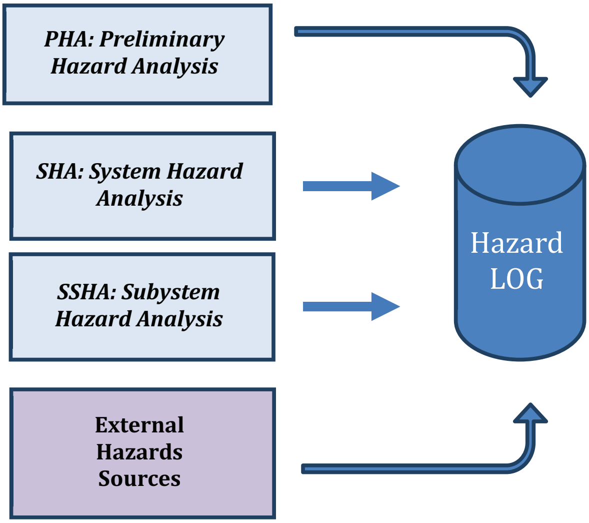

PHA: Preliminary Hazard Analysis
SHA: System Hazard Analysis
SSHA: Subsystem Hazard Analysis
External Hazards Sources
Hazard LOG

Figure 5.1 Populating the hazard log (HL).

Table 5.1 Hazard analysis template

HLS ID	Field Name	Format	Description
1	Hazard ID	A specific format has to be defined	It is the unique identifier for a hazard.
2	Hazard Opening Date	A specific format has to be defined	This field contains the date in which the hazard has been opened.
3	Hazard Closure Date	A specific format has to be defined	This field will contain the date in which the hazard closes.
4	Hazard Source	Text	Initial generic source from which the hazard was identified.
5	Hazard Description	Text	A complete exhaustive description of the hazard.
6	Hazard Cause	Text	All possible failure modes of functions/subsystems/ equipment/components which could lead to the hazard.
7	Hazard Consequence	Text	It is the possible accidents to which the hazard could lead.
8	Hazard Event	Usually each hazard is categorized following a limited list of possible hazard event, in order to ease maintenance and analysis of the results	This field reports the top level event (or a combination of events) resulting from the hazard.
9	Hazard Initial Frequency	One out of # possible values (they depends on the project, e.g., “Incredible”, “Improbable”, “Remote”, “Occasional”, “Probable,” or “Frequent”)	This field evaluates the initial frequency of the hazard, based on previous experiences, previous evaluations, expert judgment, statistical analysis and by considering the existing mitigations of legacy system and so it will be based on the data/information already available.
10	Hazard Initial Severity Level	One out of # possible values (they depends on the project, e.g., “Catastrophic”, “Critical”, “Marginal” or “Insignificant”)	This field evaluates the severity of the consequences related to the hazard, based on previous experiences, previous evaluations, expert judgment, statistical analysis and by considering the existing mitigations of legacy system and so it will be based on the data/information already available.

11	Hazard Initial Risk Valuation	One out of # possible values (they depends on the project, e.g., “Undesirable”, “Intolerable”, “Tolerable” or “Negligible”)	It is the combination of initial consequence and initial frequency. It establishes the level of risk generated by the hazardous event.
12	Hazard Final Frequency	One out of # possible values (they depends on the project. e.g., “Incredible”, “Improbable”, “Remote”, “Occasional”, “Probable” or “Frequent”)	In this field we report the final residual frequency of the hazard.
13	Hazard Final Severity Level	One out of # possible values (they depends on the project. e.g., “Catastrophic”, “Critical”, “Marginal” or “Insignificant”.)	This field evaluates the final residual severity of the consequences related to the hazard.
14	Hazard Final Risk Evaluation	One out of # possible values (they depends on the project. e.g., “Undesirable”, “Intolerable”, “Tolerable” or “Negligible”)	It is the final combination of residual consequence and frequency.
15	Hazard Status	One out of four possible values: “Open”, “Solved”, “Deleted” or “Closed”.	It is the status of hazard.

Table 5.2 An example configuration of hazard log tool ("Hazard Log Field" are the fields in DOORS, "HA" is the fields in Excel, and "Type" indicates where the field can be found (HZ, 'hazard'; MT, 'mitigation'; BH, 'can be found in both')

Hazard Log (HL) Field	Type	HA	Id
Hazard Log Id	BH	Hazard Log Id	1
Hazard Opening Date	HZ	Hazard Opening Date	2
Hazard Revision Id	HZ	Hazard Revision Id	3
Hazard Closure date	HZ	Hazard Closure date	4
Hazard Consequence	HZ	Hazard Consequence	5
Hazard Frequency Pre Mitigation	HZ	Hazard Frequency Pre Mitigation	6
Hazard Status	HZ	Hazard Status	7
Mitigation Id	BH	Mitigation Id	8
Mitigation status	MT	Mitigation status	9

Table 5.3 Example configuration for Excel scripts

Hazard Frequency Pre Mitigation	Hazard Severity Level Pre Mitigation	Hazard Risk Evaluation Pre Mitigation
	Allowed Words	
F0-Frequent	S4-Disastrous	Intolerable
F1-Probable	S3-Catastrophic	Undesirable
F2-Occational	S2-Critical	Tolerable
F3-Remote	S1-Marginal	Negligible

evaluation tool. This template is designed in MS-Excel, which allows running of scripts/macros. These macros are written considering requirements of the project.

The database consists of a collection of HZ records (one record for each identified HZ) and a collection of the mitigation action records related to the identified HZs. Each HZ record contains the information regarding the HZ such as: Hazard identification, Hazard Revision Number, Identified in phase, Hazard originator's code, Operating mode, Hazard description, etc., as per the company and project specific standard. Also, the systems and subsystems have to identify all necessary mitigations to the identified HZs so the associated risk is eliminated or ALARP (as low as reasonably practicable) according to the risk categories definitions and as explained in the safety cases. For each HZ, mitigation actions are specified to control the risk to ALARP. Each mitigation record contains information such as: Mitigation ID, Mitigation Revision, Mitigation Revision date, Mitigation Description, Applied to phase, Mitigation Status, etc. Since, each project has different needs, check of data consistency and correctness rules are needed to generate correct HL. Hence, a template and set of rules are created in MS-Excel. The rules are based on high-level requirements of standards of company in charge of HZ management, written in the form of scripts [8]. Each participant receives the template, and it is filled out with HZ data and it is thoroughly checked with Excel scripts (Figure 5.2, Figure 5.3, Figure 5.4, Figure 5.5). Once all checks are passed, it is compliant with the company and project standards. It is then sent to a central place to merge and form the *HL*. The merging of data from Excel format to DOORS is done through custom scripts which validates the data columns for correctness and consistency (Figure 5.6). Each HZ data from a participant is checked for consistency using scripts in DOORS and are integrated to form HL if no errors are found. Often Excel file consist of more fields than that of DOORS, they are either discarded or used for computation. A second script checks if a previous version of the file was uploaded yet, in such case HL is updated. Finally, the HZ log sheet is produced containing: Hazard identification, Hazard revision number, Hazard originator's Code, Hazard description, Hazard Owner, Party to act, Hazard Comments, Mitigation Comments, etc. Several fields are marked as NULL; as they will be entered during the lifetime of the system.

The cost-effectiveness of the HL management process has been achieved by the following scripts:

(i) Scripts to be used jointly with MS Office tool suite in order to make simple checks, and to reduce the number of errors introduced into the DOORS DB;

(ii) Scripts to be used in DOORS in order to ease import from excel file, update and export. Concerning the support for MS Office, the scripts were created implementing the following checks of interest for an HL:

- Concerning the hazards:
  - each hazard shall have a unique identifier;
  - each hazard shall have a non-empty "consequences", "causes", and "status";
  - each not cancelled hazard shall have a risk evaluation pre-mitigation;
  - each not cancelled hazard having a risk level pre-mitigation higher than tolerable shall have a risk evaluation post-mitigation;
  - when risk evaluation is applied the risk matrix shall be respected;
  - each hazard having status different from "cancelled" or "open" shall have a mitigation.

- Concerning the mitigations:
    - each mitigation shall have a unique identifier;
    - each mitigation shall have a non-empty “description”, “assigned to”, “status”.
- Concerning the traceability:
    - if “Mitigation Implementation (reference)” field is not empty, check trace on document list;
    - if “SRAC” field is not empty, check trace on SRAC list;
    - if “RTM” field is not empty, check trace on RTM list;
    - in case of structured HL (i.e. HZ and mitigation separated tables) – coherence checks like:
        - Does the mitigation referred in HZ table have at least an existing HZ?
        - Does all the mitigations referred in HZ table exists in the mitigation table?

5.3 Case Study

The proposed approach has been applied to four different critical projects where each project has 6–10 suppliers, and each supplier produced HZ analysis with 200–400 rows and the merged HL of ∼2000 rows for each project.

In order to evaluate the correctness and the improvement given by the scripts, we used them in different real project in order to appreciate how it is used by different teams working on different contexts. In particular we used four projects related to the Railway domain, concerning metro lines to be installed in different cities.

The main characteristic of the different project are shown in the below table.

Metro Line	Team Size	No. of Involved Subsystems	Project Duration	No. of Hazards Composing the HL
Metro X01	3	9	2015–2016	∼1600
Metro X02	4	10	2015–on going	∼2000
Metro X03	3	8	2015–on going	∼1400
Metro X04	5	10	2014–on going	∼2500

Scripts have been used during the different phases of the safety lifecycle. The scripts related to MS Office have used in the early stages to evaluate first drafts (/releases) of the files coming from suppliers. The feedbacks from the different teams are quite similar:

(i) No. of syntactic errors contained in the files given by the suppliers are drastically reduced (90%);
(ii) Time spent in reviewing (just from syntactic point of view) is drastically reduced (70%);
(iii) This goal has not been reached in a single step, indeed most of the suppliers complained on the low usability of the scripts. This is something we expected indeed they are just first releases to have feedback "from the field", so the user interface was not good enough to be reasonably used without some initial difficulties.

Scripts related to MS Office have been then used to verify correctness of the integrated HL (the one composed joining the different HAs from suppliers). Scripts related to DOORS have been used to import system HL in DOORS. In this case, feedbacks from the different teams differs. Most of the teams noticed a real improvement in using such scripts, since they:

(i) reduce time related to import activities;
(ii) make people, who are not familiar with DOORS, capable to easily use it; and
(iii) reported a real decrease in time connected with import activities (up to 80%).
(iv) One team reported no real improvement in using such scripts. This is because:
    (a) people present in the team are very skilled on DOORS (they already have their own processes to easily import HAs on it);
    (b) the presence of template for HA are really hard to be managed. This led a lot of error related to configuration of the script, which took more time to be solved.

Scripts related to DOORS have also been used to update HL. In this case, feedbacks from the teams were not so good. Indeed, most of them reported difficulties in applying the process to be used in order to correctly keep track of the different change in HL. This has led us to re-consider this phase from the scratch and changing such approach in the future projects.

5.4 Conclusion

As HL is the database for all HZ/risk information and is updated throughout the project life-cycle, it is critical that the HZ analysis data is correctly and consistently merged. Especially, in large projects having multiple partners/vendors. In the current study, the proposed approach has been found to be useful in reducing mistakes in HZ analysis. Also, it has been found to reduce the amount taken to create the HL. The use of automatic checks paves the way for correct tracking of risk and HZ analysis activities for large critical projects. More specifically:

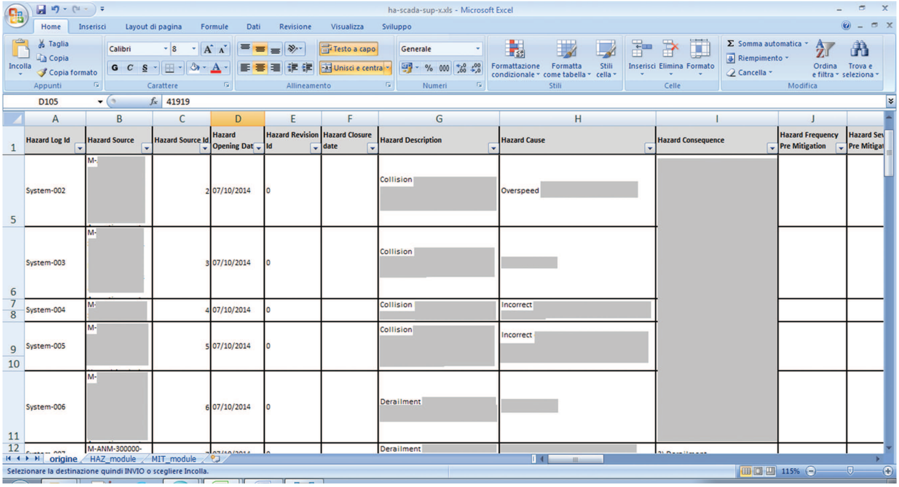
(i) All the excel sheets from all participants have been automatically imported into the DOORS tool;

(ii) It has been observed that a significant reduction in the number of non-conformities presents in the document provided by the different suppliers.

(iii) The time required to merge data to form HL is reduced by ∼30%.

(iv) Engineers in the main company are now more likely to use DOORS, since the offered framework, allowing them to easily interact with it. This also resulted in increase in quality of the project. The proposed approach has been found to be generic and suitable to all critical systems.

5.5 Tool Screenshots



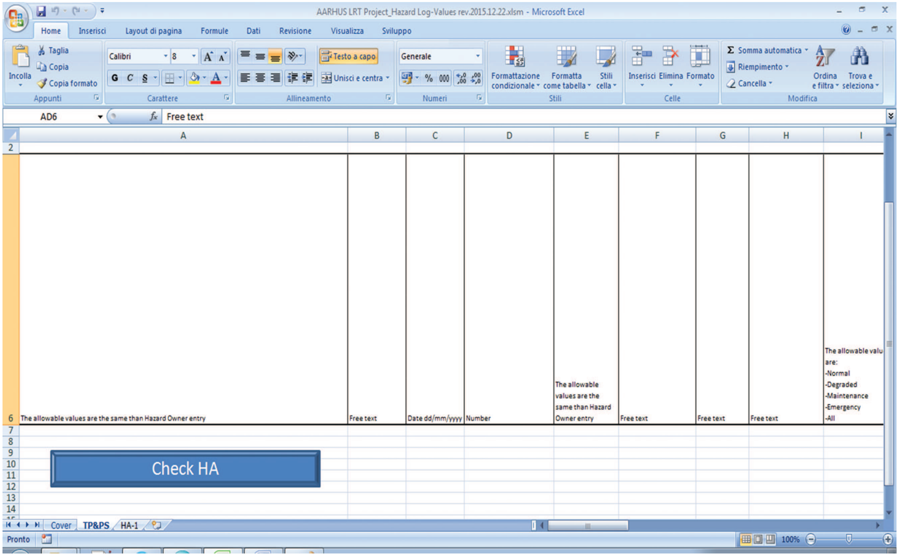
D105 | 41919

	A	B	C	D	E	F	G	H	I	J	
1	Hazard Log Id	Hazard Source	Hazard Source Id	Hazard Opening Dat	Hazard Revision Id	Hazard Closure date	Hazard Description	Hazard Cause	Hazard Consequence	Hazard Frequency Pre Mitigation	Hazard Sev Pre Mitigat
5	System-002	M-[redacted]	2	07/10/2014	0		Collision [redacted]	Overspeed [redacted]	[redacted]		
6	System-003	M-[redacted]	3	07/10/2014	0		Collision [redacted]	[redacted]			
7 8	System-004	M-[redacted]	4	07/10/2014	0		Collision [redacted]	Incorrect [redacted]			
9 10	System-005	M-[redacted]	5	07/10/2014	0		Collision [redacted]	Incorrect [redacted]			
11	System-006	M-[redacted]	6	07/10/2014	0		Derailment [redacted]	[redacted]			
12		M-ANM-300000-					Derailment [redacted]	[redacted]			

origine | HAZ_module | MIT_module

Selezionare la destinazione quindi INVIO o scegliere Incolla.

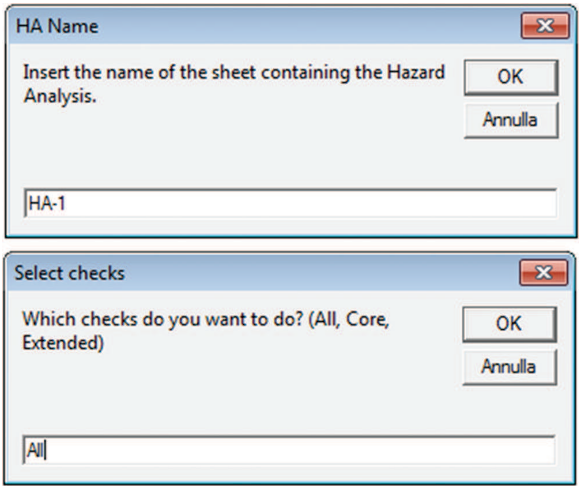
Figure 5.2 Excel sheet of one of the participants.



AD6 *fx* Free text

	A	B	C	D	E	F	G	H	I
2									
6	The allowable values are the same than Hazard Owner entry	Free text	Date dd/mm/yyyy	Number	The allowable values are the same than Hazard Owner entry	Free text	Free text	Free text	The allowable valu are: -Normal -Degraded -Maintenance -Emergency -All

Figure 5.3 Checking of HA data through MS Excel scripts.



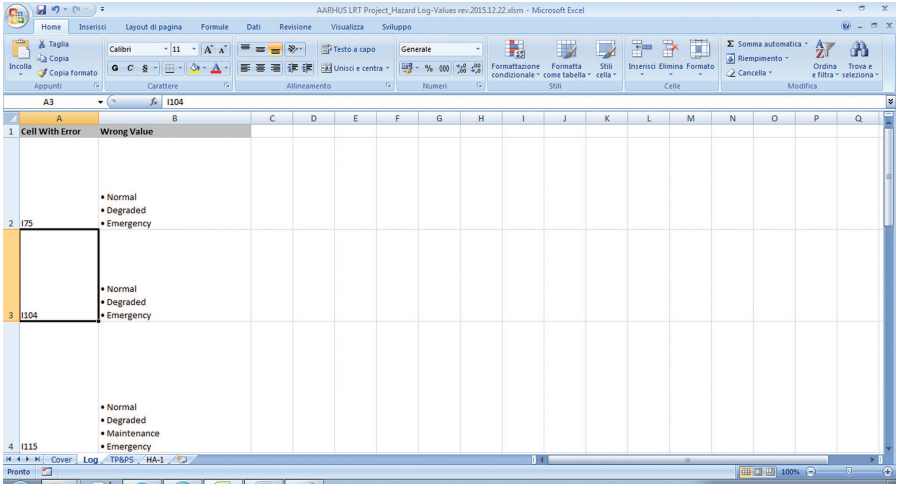
Insert the name of the sheet containing the Hazard Analysis.

HA-1

Which checks do you want to do? (All, Core, Extended)

All

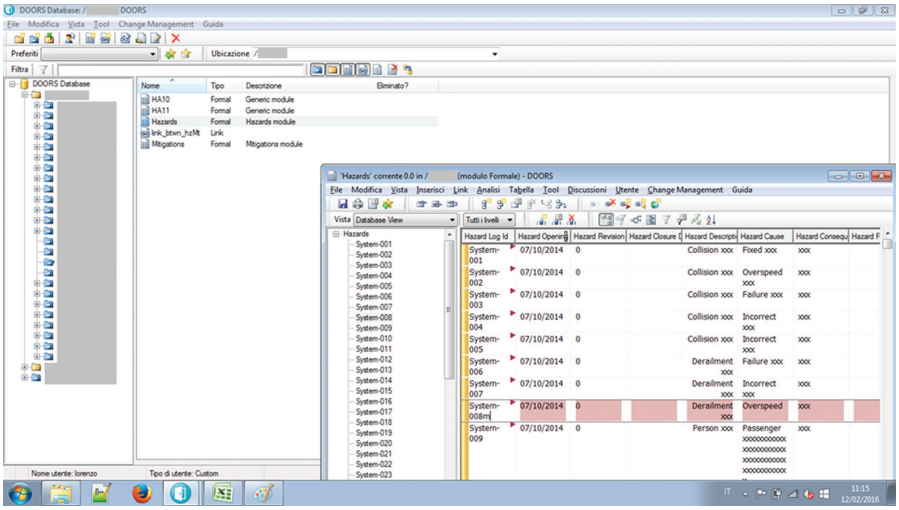
Figure 5.4 Dialogue boxes of MS Excel scripts.



A3 | I104

Cell With Error	Wrong Value
I75	• Normal • Degraded • Emergency
I104	• Normal • Degraded • Emergency
I115	• Normal • Degraded • Maintenance • Emergency

Figure 5.5 Errors caught in HZ analysis by scripts.



Ubicazione / [redacted]

Nome	Tipo	Descrizione	Eliminato?
HA10	Formal	Generic module	
HA11	Formal	Generic module	
Hazards	Formal	Hazards module	
link_btwn_hzMt	Link		
Mitigations	Formal	Mitigations module	

Vista: Database View

Hazard Log Id	Hazard Openin	Hazard Revision	Hazard Closure D	Hazard Descripti	Hazard Cause	Hazard Consequ	Hazard F
System-001	07/10/2014	0		Collision xxx	Fixed xxx	xxx	
System-002	07/10/2014	0		Collision xxx	Overspeed xxx	xxx	
System-003	07/10/2014	0		Collision xxx	Failure xxx	xxx	
System-004	07/10/2014	0		Collision xxx	Incorrect xxx	xxx	
System-005	07/10/2014	0		Collision xxx	Incorrect xxx	xxx	
System-006	07/10/2014	0		Derailment xxx	Failure xxx	xxx	
System-007	07/10/2014	0		Derailment xxx	Incorrect xxx	xxx	
System-008m	07/10/2014	0		Derailment xxx	Overspeed	xxx	
System-009	07/10/2014	0		Person xxx	Passenger xxxxxxxxxxx xxxxxxxxxxx xxxxxxxxxxx xxxxxxxxxxx	xxx	

Figure 5.6 Excel sheet imported and merged in DOORS to form HL.

References

[1] IBM. (s.d.). (*Rational DOORS Family*). Available at: http://www-03.ibm.com/software/products/en/ratidoorfami (accessed on 15 February 2016).

[2] Dave, H., and Saeed, B. (2009). "Hazard Management with DOORS: Rail Infrastructure Projects," in *Safety-Critical Systems: Problems, Process and Practice* (London: Springer), 71–93.

[3] Çakmak, K. M. (2013). Managing DO-178 Compliance with IBM Rational Platform. *J. KONBiN*, 25, 59–74.

[4] Lööf, R., and Pussinen, K. (2014). *Visualisation of requirements and their relations in embedded systems*. Uppsala University. Sweden.

[5] Dibbern, J., Geisser, M., Hildenbrand, T., and Heinzl, T. (2009). Design, implementation, and evaluation of an ICT-supported collaboration methodology for distributed requirements determination. Working paper.

[6] Pasquale, T., Rosaria, E., Pietro, M., Antonio, O., and Segnalamento Ferroviario, A. (2003). "Hazard analysis of complex distributed railway systems," in *Proceedings of 22nd International Symposium on Reliable Distributed Systems, 2003*, 283–292. doi: 10.1109/RELDIS.2003.1238078

[7] Chapra, S. (2003). *Power Programming with VBA/Excel*. Upper Saddle River, NJ: Prentice Hall.

[8] Gowen, L. D., Collofello, J. S., and Calliss, F. W. (1992). "Preliminary hazard analysis for safety-critical software systems," in *Eleventh Annual International Phoenix Conference on Computers and Communication [1992 Conference Proceedings]*, Scottsdale, AZ, USA, 1992, 501–508. doi: 10.1109/PCCC.1992.200597