European Railway Agency	

Guide for the application of the Commission Regulation (EU) N°1078/2012 on the CSM for monitoring

Reference in ERA:	ERA-GUI-05-2012-SAF
Version in ERA:	1.0
Date:	17/07/2014

Document elaborated by	European Railway Agency Rue Marc LEFRANCQ, 120 BP 20392 F-59307 Valenciennes Cedex France
Document Type:	Guide
Document Status:	Public

	Name	Function
Released by	Marcel VERSLYPE	Executive Director
Reviewed by	Christopher CARR Jean-Marie DECHAMPS	Head of Safety Unit Head of Management Sector
Written by (Author)	Antonio D'AGOSTINO Dragan JOVICIC	Safety Unit - Project Officer Safety Unit - Project Officer

DOCUMENT INFORMATION

Amendment Record

Table 1: Status of the document.

Version Date	Author(s)	Section Number	Modification Description
Version 0.16 18/07/2012	Susanne KALLMANN	All	First version of the document transmitted to the CSM working group for Formal Review.
Version 0.22 11/10/2013	Antonio D'AGOSTINO Dragan JOVICIC	All	• Guidance on the requirements contained in the Articles and the Annex of the Regulation 1078/2012 on the CSM for monitoring rewritten based on the review comments from the Danish NSA and independent railway undertakings; • Examples contained in the appendices restructured and clarified from the language point of view.
Version 0.23 18/12/2013	Antonio D'AGOSTINO Dragan JOVICIC	All	• Document updated following a Formal Review Process on version 0.22 of the document by the working group on the CSM for monitoring. Phone calls took place with those reviewers who wanted to bring additional clarifications about some of their comments.
Version 0.25 25/02/2014	Antonio D'AGOSTINO Dragan JOVICIC	All	Document updated following a Formal Review Process by the legal service of the European Railway Agency.
Version 1.0 17/07/2014	Antonio D'AGOSTINO Dragan JOVICIC	All	• Document updated with the comments of Christopher CARR, Head of Safety Unit of the Agency. • **First official version of the document published on the Agency website**

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table of Contents

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

List of Figures

List of Tables

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0. INTRODUCTION

0.1. Scope of this document

0.1.1. This document provides guidance on the application of the Commission Regulation (EU) N°1078/2012 on the common safety method (CSM) for monitoring {Ref. 2}, referred to here-after "CSM for monitoring".

0.1.2. This document does not contain any legally binding requirements. It represents the views of the European Railway Agency and not those of other EU institutions and bodies. It is without prejudice to the decision-making processes foreseen by the applicable EU legislation. Furthermore, a binding interpretation of EU law is the sole competence of the Court of Justice of the European Union.

0.1.3. This document contains only explanatory information of potential help for concerned users who directly or indirectly need to apply the CSM for monitoring. It may serve as a clarification tool however without dictating in any manner mandatory procedures to be followed and without establishing any legally binding practice. This document provides explanations on the provisions contained in Regulation (EU) N°1078/2012 and should be helpful for the understanding of the legal requirements described therein. Actors may continue to use their own existing methods for the compliance with Regulation (EU) N°1078/2012 on the CSM for monitoring.

0.1.4. The monitoring activities, strategy, priorities and plan(s) need to be adapted to the specific activities of every actor who is concerned by Regulation (EU) N°1078/2012 on the CSM for monitoring.

0.1.5. The guide document needs to be read and used together with the Regulation (EU) N°1078/2012 on the CSM for monitoring to facilitate its understanding and application. It does not replace or otherwise amend the Regulation.

0.2. Outside the scope of this document

0.2.1. This guide does not provide detailed guidance on how to carry out any specific task within the monitoring process. The guide neither provides any specific indicators which must be used nor any solutions on what actions to take when specific non-compliances are detected.

0.2.2. This guide does not define in detail the contractual agreements and arrangements that can exist between actors for the application of the CSM for monitoring. The precise content of any contractual arrangements is outside the scope of the CSM for monitoring, as well as of this guide.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.3. Structure for this guide

0.3.1. Although the guide may appear to be a standalone document for reading purposes, it does not substitute the Regulation {Ref. 2}. For ease of reference, each article of the CSM for monitoring is copied in the guide. Guidance is then provided in the following sections to help with understanding where this is considered necessary.

0.3.2. The articles and their underlying paragraphs from the Regulation on CSM for Monitoring are copied in a text box in the present guide using the "Bookman Old Style" Italic Font, the same as the present text. That formatting enables to easily distinguish the original text of the CSM for Monitoring from the additional explanations provided in this document.

0.3.3. The last part of the document contains examples of monitoring processes and activities. They shall only be considered as examples and should not be copied into an organisation without analysing the specific circumstances of the organisation.

0.4. Document description

0.4.1. The document is divided into the following parts:

(a) **Introduction**: it explains the scope of the guide and provides the list of reference documents;

(b) **Explanation of the articles of the Regulation on the CSM for monitoring**: it gives guidance on the requirements contained in the articles of the Regulation;

(c) **Explanation of the monitoring process in the Regulation on CSM for monitoring**: it gives guidance on the requirements contained in the Annex of the Regulation;

(d) **Appendices with illustrative examples of different steps of the monitoring process**: this part contains a collection of examples from European railway sector, relating to one or more parts of the CSM for monitoring.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.5. Reference documents

Table 2: Table of reference documents.

{Ref. N°}	Title	Reference	Version
{Ref. 1}	Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive)	Directive 2004/49/EC OJ L 164, 30.4.2004, p. 44, as corrected by OJ L 220, 21.6.2004, p. 16.	-
{Ref. 2}	Commission Regulation (EU) No 1078/2012 of 16 November 2012 on a common safety method for monitoring to be applied by railway undertakings, infrastructure managers after receiving a safety certificate or safety authorisation and by entities in charge of maintenance	Regulation (EU) N°1078/2012 OJ L 320, 17.11.2012, p. 8.	-
{Ref. 3}	Application guide for the design and implementation of a Railway Safety Management System	ERA/GUI/01-2011/SAF	Version 1 13/12/2010
{Ref. 4}	SMS related terminology – Application guide for the design and implementation of a railway Safety Management System	ERA/GUI/02-2011/SAF	Version 1 13/12/2010
{Ref. 5}	RSD and other management standards – Application guide for the design and implementation of a railway Safety Management System	ERA/GUI/03-2011/SAF	Version 1 13/12/2010
{Ref. 6}	Internal audits – Application guide for the design and implementation of a railway Safety Management System	ERA/GUI/04-2011/SAF	Version 2 24/05/2011
{Ref. 7}	Building knowledge texts – Application guide for the design and implementation of a railway Safety Management System	ERA/GUI/05-2011/SAF	Version 1 13/12/2010
{Ref. 8}	Guide for the application of the Commission Regulation No 445/2011 on a system of certification of entities in charge of maintenance for freight wagons	ERA/GUI/08-2011/SAF	0.5
{Ref. 9}	ECM certification - Application guide including explanations on ECM certification scheme	ERA/GUI/09-2011/SAF	1.0
{Ref. 10}	ECM certification - Application guide with additional explanations on Sectorial Accreditation Scheme	ERA/GUI/10-2011/SAF	1.0
{Ref. 11}	ECM certification - Application guide including explanations on maintenance workshop certification scheme	ERA/GUI/11-2011/SAF	1.0
{Ref. 12}	ECM accreditation and certification schemes - Explanatory document	-	Version 1.0 21/10/2011
{Ref. 13}	Commission Regulation (EU) No 445/2011 of 10 May 2011 on a system of certification of entities in charge of maintenance for freight wagons and amending	Commission Regulation (EU) N°445/2011 OJ L 122; 11.5.2011, p.22.	10 May 2011
{Ref. 14}	Commission implementing Regulation (EU) N°402/2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009	Commission Regulation (EU) N°402/2013 OJ L 121; 3.5.2013, p.8	30 April 2013

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.6. Standard definitions, terms and abbreviations

0.6.1. Specific safety management system related terminology is explained in {Ref. 4}.

0.6.2. New definitions, terms and abbreviations in this guide are defined in Table 3, Table 4 and Article 2.

0.7. Specific definitions

0.7.1. See Article 2.

0.8. Terms and abbreviations

0.8.1. This section defines the new specific terms and abbreviations that are used frequently in the present document.

Table 3: Table of terms.

Term	Definition
Agency	The European Railway Agency (ERA)
Guide	The present document "Guide on CSM for monitoring"

Table 4: Table of abbreviations.

Abbreviation	Meaning
CSM	Common Safety Method
CSI	Common Safety Indicator
EC	European Commission
ECM	Entity in Charge of Maintenance
ERA	European Railway Agency
FMEA	Failure Mode and Effect Analysis
IM	Infrastructure Manager
NSA	National Safety Authority
RSD	Railway Safety Directive
RU	Railway Undertaking
SMS	Safety Management System

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

EXPLANATION OF THE ARTICLES OF THE REGULATION

Article 1. Subject-matter and scope

Article 1 (1)

This Regulation establishes a common safety method (CSM) for monitoring, enabling the effective management of safety in the railway system during its operation and maintenance activities and, where appropriate, improving the management system.

[G 1] To fulfil the obligations in Article 4(3), Article 9 and Article 14a(3) of Directive 2004/49/EC:

(a) railway undertakings and infrastructure managers have to establish safety management systems to ensure a safe operation of the railway system, a safe traffic management and the control of risks associated to them;

(b) entities in charge of maintenance have to establish a system of maintenance to ensure that the vehicles for which they are in charge of maintenance are in the design operating state.

Knowing that a "safety management system" and a "system of maintenance" *(both designated by "management system" in definition (a) of Article 2 of the CSM for monitoring – see also guidance on Article 2 in this document)* is a documented set of processes, procedures and risk control measures, their appropriateness to actually control the risks of railway undertakings, infrastructure managers and entities in charge of maintenance needs to be verified continuously in its correct implementation and effectiveness.

[G 2] The purpose of the CSM for monitoring is therefore to provide a harmonised method to verify that:

(a) the processes, procedures and risk control measures contained in the management system are applied correctly and are effective, and that;

(b) the company safety targets and objectives are achieved in practice, i.e. during the operation and maintenance activities.

[G 3] The purpose of the CSM for monitoring is also to continuously improve, where reasonably practicable, either the management system or the safety performances.

[G 4] As consequences of points [G 2] and [G 3], the monitoring activities are architectured around the "monitoring process" itself and the "continuous improvement". A visual description is given in Figure 1.

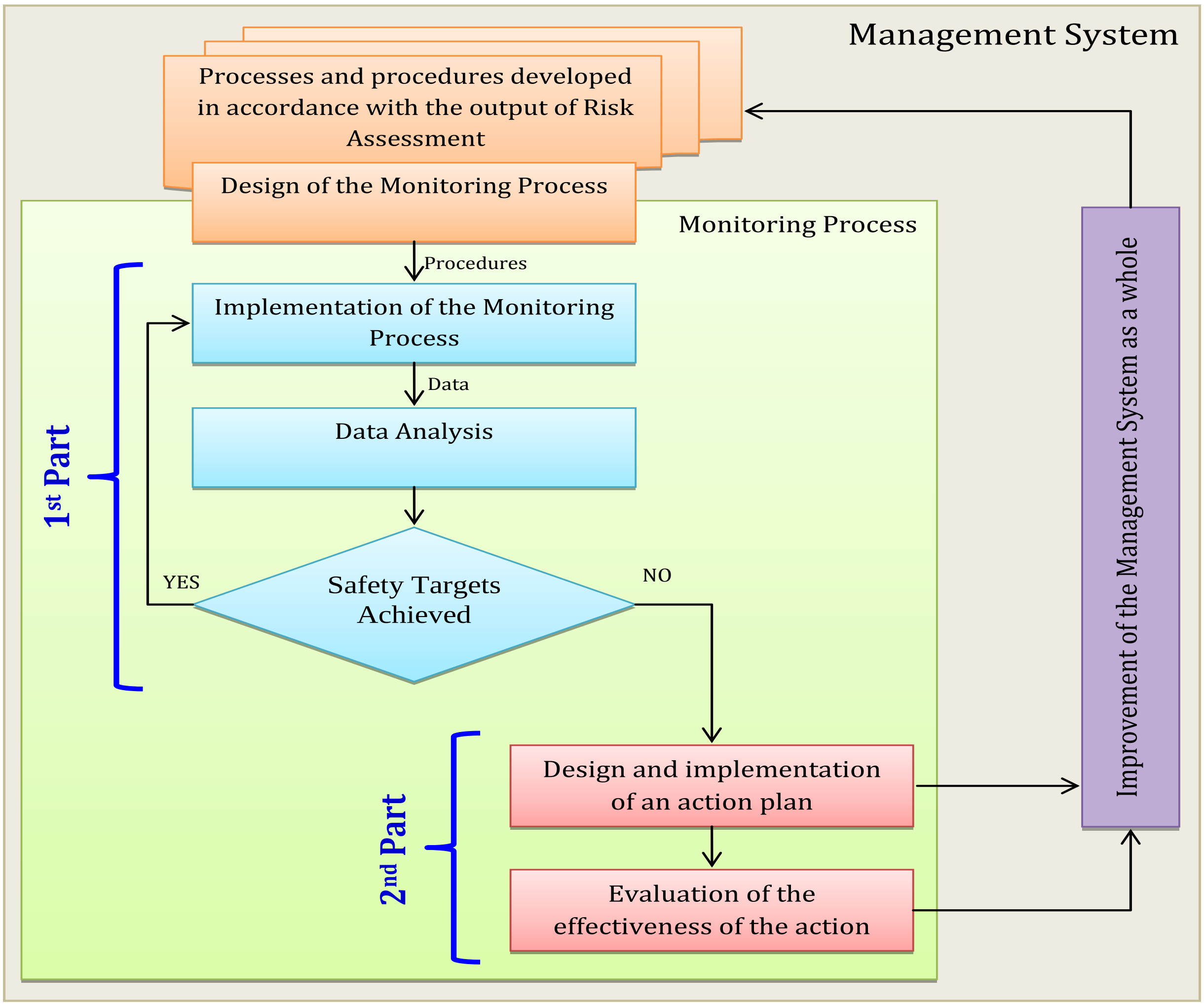


Figure 1: The structure of the CSM for monitoring

[G 5] The CSM for monitoring does not introduce novelties in the field of the management systems, but defines a harmonised framework to monitor and improve a management system of those actors who fall under the scope of the Railway Safety Directive 2004/49/EC (i.e. railway undertakings [RUs], infrastructure managers [IMs] and entities in charge of maintenance [ECMs]).

[G 6] Guidance on the safety management system for railway undertakings and infrastructure managers is available in {Ref. 3}. Guidance for the system of maintenance of entities in charge of maintenance is available in {Ref. 8}.

[G 7] For guidance on "*where appropriate, improving the management system*" see explanations in sections 3 and 4 for the Annex of the CSM for monitoring.

Article 1 (2)

This Regulation shall be used for the following:

(a) to check the correct application and the effectiveness of all the processes and procedures in the management system, including the technical, operational and organisational risk control measures. In case of railway undertakings and infrastructure managers checking will include the technical, operational and organisational elements that are necessary for the delivery of the certification specified on the Article 10.2(a) and 11.1(a) and the provisions adopted to obtain the certification specified on the Article 10.2(b) and 11.1(b) of Directive 2004/49/EC;

(b) to check the correct application of the management system as a whole, and if the management system achieves the expected outcomes, and;

(c) to identify and implement appropriate preventive, corrective or both types of measures if any relevant instance of non-compliance to points (a) and (b) is detected.

More about "checking the correct application and the effectiveness of all processes and procedures in the management system"

[G 1] The management system in place in railway undertakings, infrastructure managers and entities in charge of maintenance is based on processes. One part of the management system is the process for monitoring the correct application and the effectiveness of:

(a) on one side, all the processes and procedures contained in the management system, and ;

(b) on the other side, the management system as a whole.

[G 2] Article 1(2) provides elements concerning the design of the monitoring process:

(a) it specifies that ***all the processes and procedures shall be monitored***. This means that in order to comply with Article 3 (2)(a), every process and procedure contained in the management system needs to be considered for defining the strategy, priorities and plan(s) for monitoring. These concepts are further developed in the explanation of the Annex of the CSM Regulation;

(b) it makes the distinction between the concept of "**correct application"** and the concept of "**effectiveness"**.

[G 3] To better explain the difference between **correct application** and **effectiveness** let us consider an example:

Example 1:

Assume a railway undertaking uses a procedure which describes a set of checks to be done by the driver when taking in charge the rolling stock.

This procedure is a unique[(1)] risk control measure in the management system to control the occurrences of the following unwanted events[(2)]:

(a) fire in rolling stock;
(b) loss of parts during the run of the train;
(c) derailments.

Assume the frequency of occurrence of the above mentioned unwanted events is represented by a specific value for which a safety target (frequency of occurrence/million train*km) is set up:

Table 5: Safety targets for unwanted events detectable by the driver checks when taking in charge the rolling stock.

Unwanted event	Frequency of occurrence	Traffic	Severity
fire in rolling stock	1*year	20 million train*km	0 fatalities
loss of parts during the run of the train	5*year	20 million train*km	0 fatalities
derailments	1*year	20 million train*km	0 fatalities

[G 4] Figure 2 represents the whole monitoring cycle for the considered example and the link between risk assessment and monitoring activities:

(a) predictive risk assessment:

(1) during the risk assessment of the activities of the railway undertaking and the setting up of its safety management system, the three unwanted events in Table 5 were identified and a safety target has been defined for each of them;

(2) a procedural risk control measure has been defined: "*set of checks to be done on the rolling stock when the driver takes it in charge*";

(3) this procedure of the safety management system is to be applied in practice by the driver when he takes in charge rolling stock;

(1) *This approach is not to be considered as good practice. This risk control measure is to be considered only as an example.*

(2) *An unwanted event can be an accident, an incident, a near-miss or any other dangerous occurrence.*

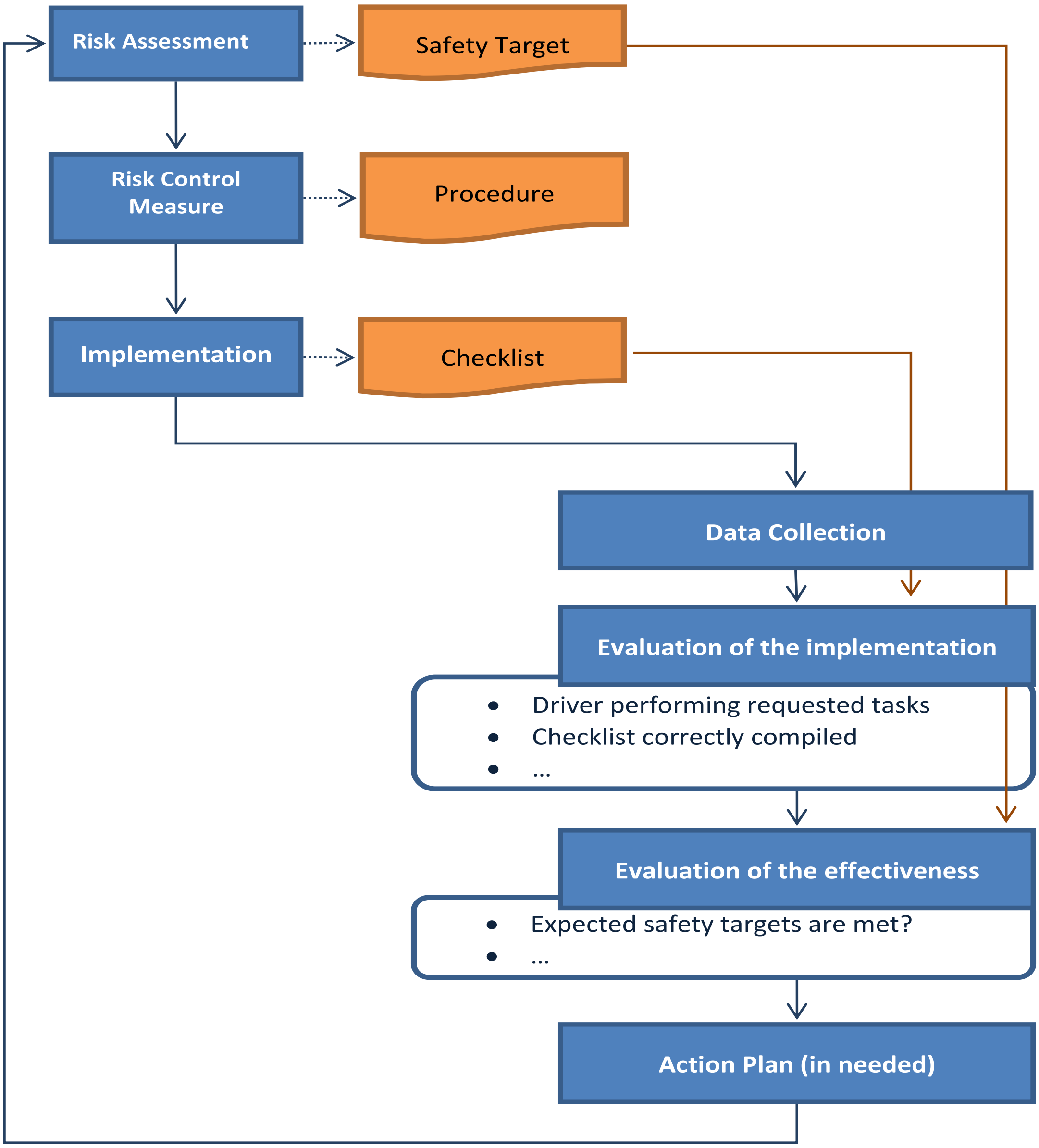


Figure 2: Simplified Monitoring cycle: check of correct application and effectiveness

(b) monitoring activities:

(1) collect monitoring information and data;

(2) verify whether the driver applies correctly the procedure, verifying all the items in the checklist of the procedure → "this corresponds to the check of the correct application of the relevant procedures of the management system";

(3) evaluate whether the safety targets specified in the management system are met → "this corresponds to the check of the effectiveness of the relevant

procedures of the management system", i.e. to verify in practice that the relevant procedure enables to keep the considered risks under control and therefore that the frequency of occurrence of the unwanted events is below the specified thresholds;

(4) if the procedure is not correctly applied by the driver or if it does not provide a sufficient level of protection, a corrective action plan is necessary.

In this case, an additional risk assessment is necessary to find out the reasons for the non-compliances and to define appropriate corrective risk control measures (action plan). The correct implementation of the action plan and the effectiveness of the measures contained in this action plan need to be monitored in a similar way as described above.

[G 5] During the predictive risk assessment a causal analysis can be done for the unwanted events (a), (b) and (c) in Table 5. It enables to identify the events (or precursors) that could "lead" to the occurrence of the unwanted events. A possible and non-exhaustive list of precursors is reported in Table 6:

Table 6: Example of precursors for the unwanted events in Table 5.

Unwanted event	Precursor	Risk Control Measure
Fire in rolling stock	Fire extinguishing system not efficient	The driver shall check the efficiency of the "fire extinguishing system" in accordance with the procedure given by the manufacturer
	Misuse of the locomotive	Establish a training process for the staff
	…	…
Loss of parts during the run of the train	Wearing of structural parts of the locomotive	The driver shall carry out defined pre-departure checks on the locomotive
	Wearing of structural parts of the wagons	The master wagon shall carry out pre-departure checks on the wagon
	Inspection doors on the body of the locomotive not properly closed.	The driver shall carry out defined pre-departure checks on the locomotive
	…	…
Derailments	Worn wheels of the locomotive	The driver shall carry out defined pre-departure checks on the locomotive
	Worn wheels of the wagons	The master wagon shall carry out pre-departure checks on the wagon
	…	…

[G 6] The causal analysis enables to specify additional safety targets based on those precursors. For example, when considering the unwanted event “fire in rolling stock”, it is known from the risk analysis that its occurrence can be influenced by a "fire extinguishing system being not efficient".

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 7] It is then possible to assume, for instance based on experience and/or statistics, that every 20 failures of the "fire extinguishing system", the unwanted event "fire in rolling stock" occurs. Consequently, a "safety target" of "less than 20 occurrences per year and per locomotive" can be set for this precursor. It is also to note that precursors do not need a severity to be assigned: see Table 7.

Table 7: Example of definition of safety targets for precursors.

Precursors	Frequency of occurrence	Traffic	Severity
…	…	…	N.A.
Fire extinguishing system not efficient	<20*year*loco	20 million train*km	N.A.
…	…	…	N.A.

[G 8] Within the considered procedure, the task of the driver is to report, in a checklist, the results of the checks he does before taking in charge the locomotive: see Table 8.

Table 8: Example of checklist.

ID	Driver's tasks	OK	NOT OK	Comments
1	Visual inspection of the bogies			
2	Visual inspection of the body of the locomotive			
3	Inspection doors closed			**Inspection door not locked**
4	Test of the fire extinguishing system of the locomotive			
…	…			
N	Visual inspection of the profile of the wheels			

Table 9: Example of a checklist fully compiled by the driver showing the correct application of a procedure of the management system.

ID	Driver's tasks	OK	NOT OK	Comments
1	Visual inspection of the bogies	✓		
2	Visual inspection of the body of the locomotive	✓		
3	Inspection doors closed		✓	**Inspection door not locked**
4	Test of the fire extinguishing system of the locomotive	✓		
…	…			
N	Visual inspection of the profile of the wheels	✓		

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 9] The procedure is **correctly applied** when the driver performs all the checks foreseen in the checklist and this is entirely followed, also in case non-conformities are reported: see Table 9.

[G 10] The procedure is **effective** if, after having checked the correct application of it, all the events, that wanted to be prevented, have an occurrence (safety performance) that is below the targets defined during the design of the procedure: see Table 10.

Table 10: Check of achievement of safety targets.

Safety Targets set up in management system				
Unwanted event	**Frequency of occurrence**	**Expected Traffic**	**Severity**	
fire in rolling stock	1	20 million train*km	0 fatalities	
loss of parts during the run of the train	5	20 million train*km	0 fatalities	
derailments	1	20 million train*km	0 fatalities	
Safety Targets set up in management system for the precursors				
Precursors	**Frequency of occurrence**	**Expected Traffic**	**Severity**	
…	…	…	…	
Fire extinguishing system not efficient	<20*year*loco	20 million train*km	N.A.	
…	…	…	…	
Measured Safety Performances				**Is safety target achieved?**
Unwanted event	**Frequency of occurrence**	**Actual Traffic**	**Severity**	
fire in rolling stock	1	19.6 million train*km	0 fatalities	YES
loss of parts during the run of the train	7	19.6 million train*km	1 injury	NO
derailments	0	19.6 million train*km	0 fatalities	YES
Measured Safety Performances				**Is safety target achieved?**
Precursors	**Frequency of occurrence**	**Actual Traffic**	**Severity**	
…	…	…	…	NO
Fire extinguishing system not efficient	5	19.6 million train*km	N.A.	YES
…	…	…	…	NO

[G 11] From Table 10 it appears that although the safety target for the "fire extinguishing system not efficient" precursor is achieved(3), the unwanted event "fire in rolling stock"

(3) *The "fire extinguishing system not efficient" precursor occurred 5 times per year and per locomotive; the associated safety target was set to "less than 20 occurrences per year and per locomotive".*

occurred. This shows that the predictive risk assessment and causal analysis were incomplete. They did not identify all combinations of causes that could lead to the occurrence of the considered unwanted event. Consequently, the monitoring of "fire extinguishing system not efficient" precursor is not sufficient to prevent the occurrence of the unwanted event (fire in rolling stock). It can thus be concluded from Table 10 that the monitoring indicators and planning can be improved.

[G 12] The checklist in Table 9 is based on a list of precursors identified during the predictive risk assessment. Such a checklist is a tool for registering precursors and reporting them to the safety department for further analyses.

[G 13] To evaluate the effectiveness of a process/procedure, it is necessary to have a correct application of it. In the case of the above mentioned procedure for train drivers, in case the unwanted event "fire in rolling stock" occurs and the procedure for the inspections is not fully and correctly implemented, it is difficult to check whether the unwanted event occurred because the procedure was not (correctly) applied or whether the procedure was not well designed and consequently could not be effective.

[G 14] It must also be pointed out that the safety targets can seem to be achieved even if the procedures are not correctly implemented. Such non-compliances with the management system processes and procedures should not be accepted because it can lead to a false perception of safety within the company. Such a case could happen when the management system has some redundant risk control measures. An investigation of why safety targets are achieved whereas non-compliances are observed can help to evaluate the right level of efficiency achieved by the management system.

[G 15] Partial or incorrect application of a procedure should **always** be reported and treated as non-compliance, even in case there are no consequences on the safety performances. For example, if:

(a) a user misreads how to carry out a task within a certain process or procedure or,
(b) a user puts in place "the wrong" risk control measure in the design and implementation of the management system or,
(c) in other ways, a user does not correctly apply the process or procedure,

the task is carried out in a different way (or under different conditions) compared to how it was initially planned and/or specified through the management system. This could result in an incorrect application of the processes and procedures that directly affects the effectiveness in mitigating or removing the associated risk(s).

[G 16] In some cases, when it is not necessary or possible to describe in detail the instructions of a procedure, the procedure could give room to a personal interpretation by the person responsible for its application. And where a procedure involves more than one actor, there is an increased margin for personal interpretation of the instructions provided by the procedure. The result could be an important deviation in the correct application of the procedure that could lead to unwanted events.

[G 17] The complexity of the procedure can be considered as criteria to prioritise monitoring when the design of the procedure cannot be improved and when many actors are involved. For further information concerning prioritisation in monitoring please consult paragraph [G 9] of chapter 2 of the explanations for the Annex of the CSM for monitoring.

[G 18] To push towards the correct application of procedures and processes, it is important to design them on the basis of the real needs of the organisation and to keep them up-to-date, taking into account their applicability by the operational staff.

More about "checking the correct application and effectiveness of the management system as a whole"

[G 19] The concept of correct application and of effectiveness, explained for the single process/procedure, can be extended to the system as a whole: see Figure 4.

[G 20] Checking the correct application or checking the effectiveness of a single or a small group of processes or procedures could give a satisfactory result, but this does not necessarily mean that all the processes and procedures together are correctly applied or that the relevant safety targets are met.

[G 21] Analysing the following process description (according to the technique IDEF0[(4)] – see also Figure 3), it shows how the output of the analysed process is dependent on:

(a) the inputs of the different sub-processes that compose the analysed process;
(b) the outputs of the different sub-processes that compose the analysed process;
(c) the interfaces among the sub-processes;
(d) the legal framework, the safety requirements and constraints;
(e) the staff responsible for the execution of the tasks.

If these were the only elements influencing the overall performance of the single process, it could have been stated that it is possible to verify the performance of the process just monitoring the elements included in it.

The "design" of the process has also a strong influence on the performance of the process.

If a process is not correctly designed, its performances will be poor (because other processes are missing), even if the sub-processes defined in it are well performing.

(4) *For further explanations about IDEFO, visit web site: http://www.idef.com/idef0.htm*

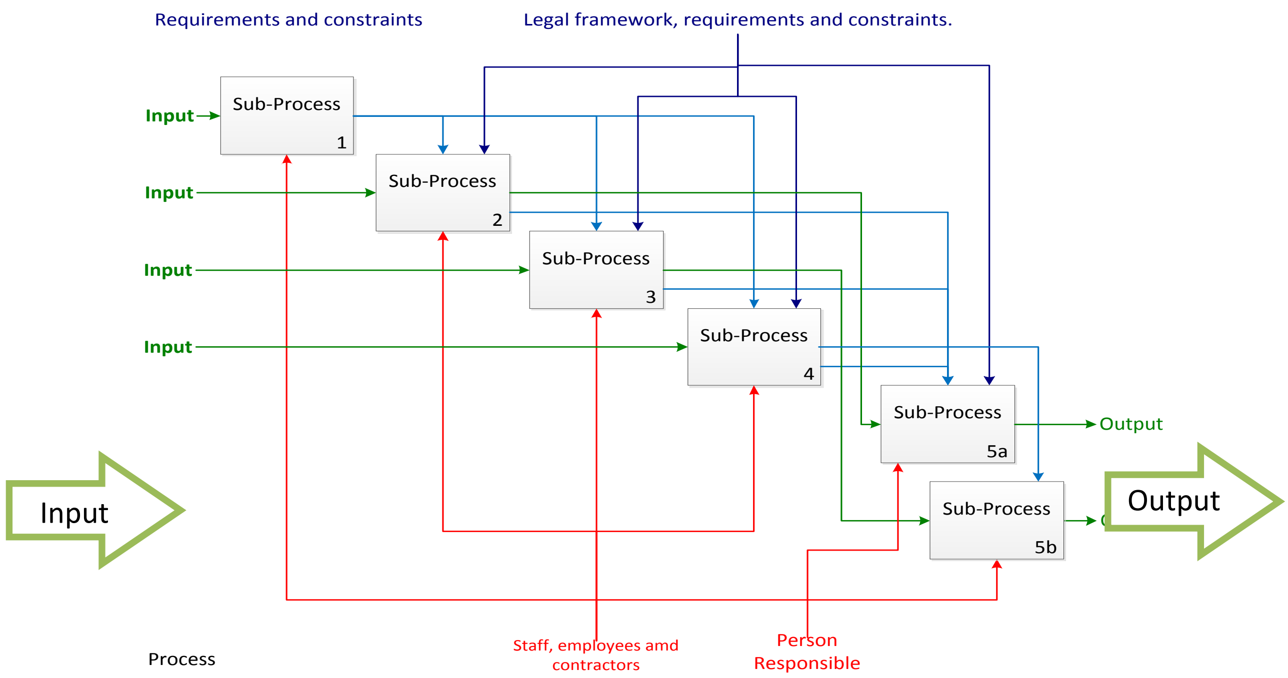


Figure 3: System view for checking the correct application and effectiveness of the management system as a whole.

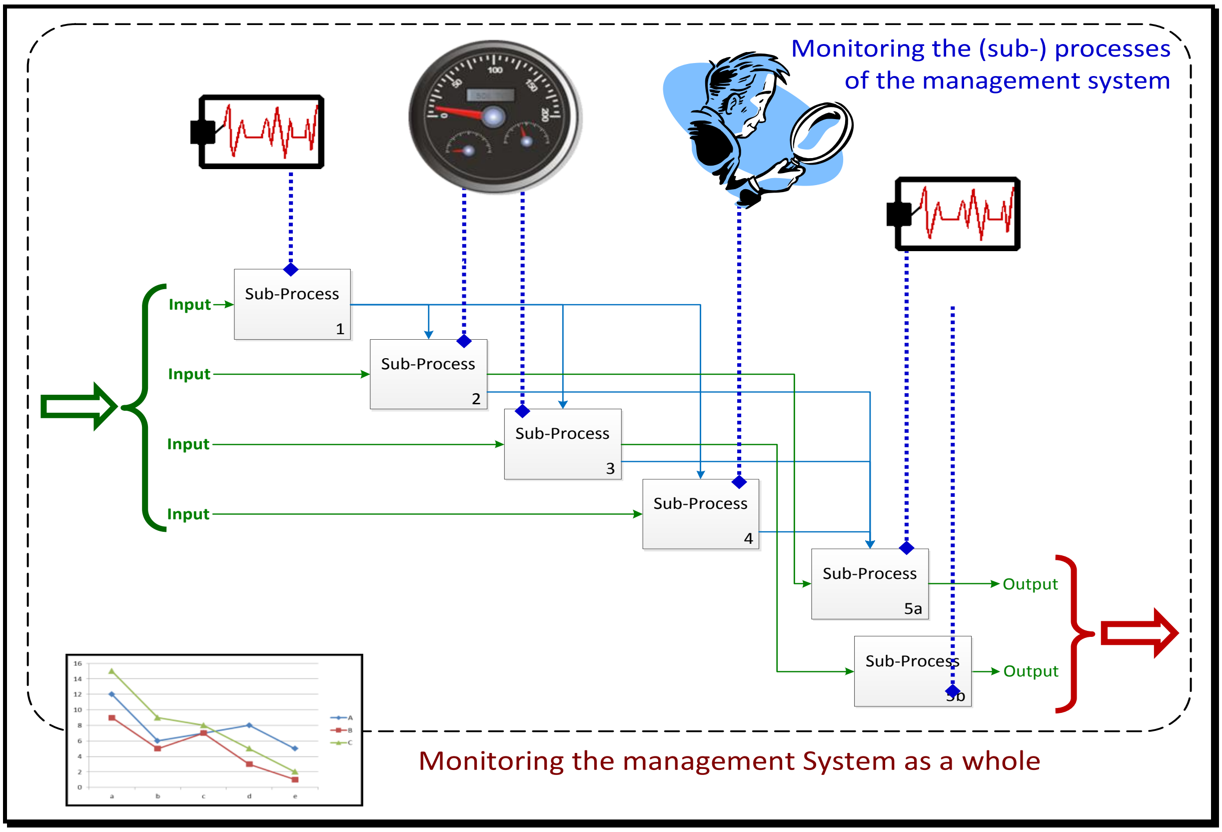


Figure 4: Monitoring the management system as a whole.

[G 22] All checks need to be in proportion to the nature and magnitude of the associated risk. See further guidance in section 2 of the explanation of the Annex in the CSM for monitoring.

[G 23] Further guidance on all the above can be found in the chapter "Explanations of the annex in the Regulation on CSM for monitoring".

More about "needs for preventive and corrective measures"

[G 24] Depending on its specific monitoring strategy, the railway undertaking, infrastructure manager or entity in charge of maintenance will thus decide, based on the analysis of the results collected from monitoring activities, whether it is necessary to implement preventive, corrective or both types of measures.

[G 25] Preventive and corrective actions should be considered when the measured safety performance is clearly lower than the expected/targeted performance.

[G 26] Safety targets can also be defined according to the strategy resulting from the safety policy of the company. They can be expressed through qualitative or quantitative values.

[G 27] Safety performances can also be expressed in a qualitative or quantitative way.

[G 28] To help the reader understand these concepts, the example below of the number of signals passed at danger (SPADs) is considered:

Element of the strategy for monitoring the safety performances of a railway under-taking:

> *"…for unwanted events with a potential for a high risk, the trend of their occurrence is a criterion to be used in the decision making process, regarding the need to define a corrective or preventive action…"*

This means that the management of the railway undertaking does not check only if the safety target related to the number of signals passed at danger (SPADs) is achieved, but it also takes into account the trend of the occurrence of this unwanted event. To measure the tendency of the safety performance for this unwanted event, it is necessary to correlate the number of SPADs to the actual number of "million train*km" [m_train*km] run during the analysed year.

These principle and concepts are illustrated by Table 11 and Figure 5.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table 11: Example of statistics for the number of SPADs.

	2006	2007	2008	2009	2010	2011
SPAD	6	6	5	4	3	2
m_train*km	2	3	4	3	2	1
Ratio	3	2	1,25	1,33	1,5	2

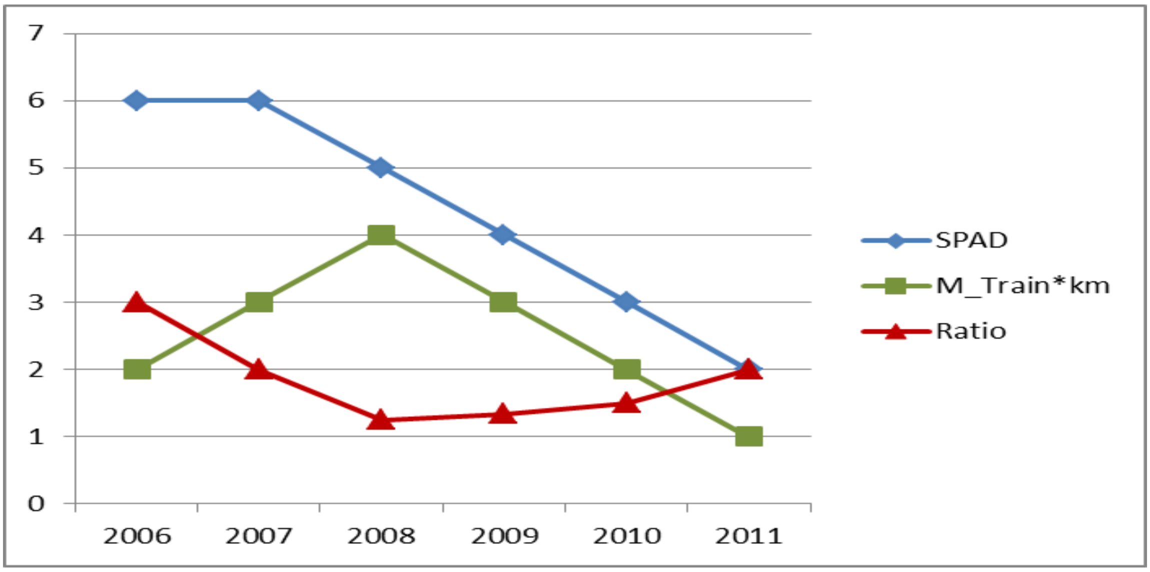


Figure 5: Example of data analysis and trend monitoring for the number of SPADs.

[G 29] Looking at the Figure 5, it is clear that from 2006 to 2008 the safety performances were improving (where it is also assumed that the safety targets are met). The report of 2008 shows a reduction in the number of SPADs but considering the reduction in terms of "million train*km" the safety performance is degraded.

[G 30] In 2008, the safety performances start to degrade. That means that the safety targets are not going to be met anymore if corrective/preventive actions are not taken.

[G 31] A signal passed at danger (SPAD) unwanted event is one of the most dangerous precursors, as in some conditions it can lead to serious accidents. As it has the potential for a high risk, the occurrence of SPADs is to be analysed according to the specified safety target and its trend during the time. Considering Figure 5, it can be concluded that if at the end of 2008, the company had decided to turn the trend around and to put in place a preventive or corrective action, the safety performance archived in 2009 could have been better than the measured outcome. An effective and proactive monitoring process should provide to the management the necessary information to act on in such a proactive manner.

Article 1 (3)

This Regulation shall apply to railway undertakings, infrastructure managers after receiving a safety certificate or safety authorisation and entities in charge of maintenance.

[G 1] According to Article 4(3) of Directive 2004/49/EC, railway undertakings and infrastructure managers are responsible *"for the safe operation of the railway system and the control of risks associated with it"*. They are also obliged to have in place a safety management system.

[G 2] According to Article 14a(3) of Directive 2004/49/EC, entities in charge of maintenance are responsible to ensure *"that the vehicles for which they are in charge of maintenance are in a safe state of running by means of a system of maintenance"*. Consequently, all entities in charge of maintenance are obliged to have in place a system of maintenance, i.e. not only the ECMs which are certified according to the ECM Regulation {Ref. 13}.

[G 3] The monitoring process is part of the management system. Therefore, procedures, processes or part(s) of them, defining the monitoring activities, need to be foreseen during the design-phase of the management system. The application of the monitoring process should then start after receiving the safety certificate, safety authorisation or the ECM certificate, i.e. during the operation and maintenance of the railway system.

Article 2. Definitions

For the purposes of this Regulation the definitions of Article 3 of Directive 2004/49/EC shall apply.
In addition, the following definitions shall apply:

*(a) **'management system'** means either the safety management systems of railway undertakings and infrastructure managers, as defined in Article 3(i) of Directive 2004/49/EC and complying with requirements laid down in Article 9 and Annex III of that Directive, or the system of maintenance of entities in charge of maintenance complying with requirements laid down in Article 14a(3) of that Directive;*

*(b) **'monitoring'** means the arrangements put in place by railway undertakings, infrastructure managers or entities in charge of maintenance to check their management system is correctly applied and effective;*

*(c) **'interfaces'** means interfaces as defined in Article 3(7) of Commission Regulation (EC) No 352/2009*[5]

[5] *OJ L 108, 29.4.2009, p. 4.*

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] For the purpose of the CSM for monitoring and to avoid duplicating the same requirements for railway undertakings, infrastructure managers and entities in charge of maintenance, it was decided to use the generic terminology "management system" as defined in point (a) of Article (2) of the CSM for monitoring. This choice makes the Regulation shorter and easier to read.

[G 2] Therefore the terminology "management system" does not require to include in the monitoring activities any other company system of management (e.g. system of quality management, environment management system, etc.) which is not meant under Articles 3(i) and 9, Annex III and Article 14a(3) of Directive 2004/49/EC {Ref. 1}.

Article 3. Monitoring process

Article 3 (1)

Each railway undertaking, infrastructure manager and entity in charge of maintenance:

(a) shall be responsible for conducting the monitoring process set out in the Annex;

(b) shall ensure that risk control measures implemented by their contractors are also monitored in compliance with this Regulation. To this end, they shall apply the monitoring process set out in the Annex or require their contractors to apply this process through contractual arrangements.

[G 1] In the previous sections of this guide, it is explained that railway undertakings, infrastructure managers and entities in charge of maintenance have the responsibility to design, implement, monitor and continuously improve their monitoring process.

[G 2] According to the Directive 2004/49/EC, even if a contractor is hired to be part of the overall operation and maintenance of the railway system, railway undertakings, infrastructure managers and entities in charge of maintenance remain responsible for ensuring that the whole monitoring chain supports the delivery of safe performance.

[G 3] Risk control measures defined in the framework of risk assessment need to be monitored. The same applies to risk control measures adopted by contractors and sub-contractors. The CSM for monitoring requires that either railway undertakings, infrastructure managers and entities in charge of maintenance apply themselves the monitoring process defined in the Annex of the CSM for monitoring, or they foresee contractual arrangements with their contractors to describe:

(a) how the monitoring activities are to be managed and shared between them;

(b) how to make available the information necessary for carrying out the monitoring activities and implementing appropriate preventive and/or corrective measures if any relevant non-compliance is detected.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 4] Indeed, in order to fulfil the requirements of Article 1 (2)(b) and Article 1 (2)(c), it is important to verify that the outsourced safety related activities also deliver the expected safety performance.

More about "monitoring the contractors"

[G 5] Monitoring contractors has a safety and business aim:

(a) from a safety point of view, the contracting entity[(6)] keeps the responsibility for the safety of the outsourced activities;

(b) from a business point of view, the contracting entity should check whether the contractor delivers the service that has been agreed on in the contract. For instance, specific requirements concerning technical characteristics of spare parts or the use of a certain number of operational staff in the execution of some safety related tasks need to be monitored. These specific requirements may represent a safety measure that can impact the business, for example by increasing the costs. The use of the monitoring process in this case supports also the business development as it enables to check that the contractual agreements are effectively delivered.

[G 6] To set up a good basis for a safe management and monitoring of the outsourced activities, a risk assessment is helpful before deciding to contract or sub-contract, totally or partially, a safety-related activity, and before signing the contract. It is good practice also to log the outcomes of the risk assessment into a safety report that should include all the necessary safety requirements.

[G 7] Instructions, technical specifications or other supporting documents should be defined, by the contracting entity, for a better design of the contractual arrangements and for supporting the contractor in delivering what is required.

[G 8] The following short example is considered to illustrate how to define the safety requirements to be included in the contractual arrangements.

> **Example 2:**
>
> A railway company decides to sub-contract an activity. This choice represents a change that is to be managed according to the procedures of the management system of the company.

(6) *Contracting entity as defined in Article 2(r) of the interoperability Directive 2008/57.*

> Remark: this example focuses only on the organisational aspects of the change. Although the technical or operational aspects of the change are also to be covered for a complete management of safety, for the purpose of this example the analysis is not included below.
>
> The organisational change consists in a redesign of the management system where some of the activities previously carried out internally in the company are going to be out sourced. A new interface is going to be created.

[G 9] In the scope of the risk assessment (that is not exhaustively documented in this document), a hazard identification is performed. The following hazards are identified for the outsourced activities:

(a) the contractor is not competent to deliver what the railway company requests;
(b) the contractor is not conscious of the impact of its work on the safety level of the railway system;
(c) the workers of the contractor are not aware of the hazards coming from the new working environment;
(d) the railway company produces instructions or contractual arrangements where there is room for interpretation;
(e) other hazards and risks (the list is not exhaustive).

[G 10] As it is not the aim of this document to illustrate a risk assessment and the application of the CSM for risk assessment {Ref. 14}, the details regarding the full risk assessment activity are not included. Only the outcomes related to the definition of the "safety requirements" are listed in Table 12.

[G 11] Based on the results of the risk assessment reported in Table 12 and looking at the "monitoring" column it is possible to develop a specific monitoring activity for the outsourced work.

[G 12] The internal process of qualification and monitoring of contractors should be monitored and improved. In order to boost the quality and the safety level of the contractors, involved in the railway activities, it is advisable that at least the following element should be monitored:

(a) the actual owning of qualification criteria (certifications, quality management, etc.);
(b) the maintenance of the qualification criteria for the whole length of the contract.

[G 13] These checks can be undertaken on a documental basis, through audits, inspections, etc.

[G 14] This process facilitates the investigation of the root causes of an accident, incident or near miss involving a contractor.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table 12: Example of FMEA for an outsourced activity.

Hazard	Consequences	Safety requirement	Demonstration of compliance	Monitoring activity
The contractor is not competent to deliver what the railway company requests	Service delivered by the contractor is not compliant with the contractual technical and safety requirements	1. Define a company "procedure for selecting qualified contractors according to an internal qualification scheme" including: (a) assessment of competence; (b) certifications (e.g. ISO 9001 or ECM certificate); (c) proven experience in the same type of services or activities for another customer.	A procedure is defined according to both the company document management system and the organisation of the company. Selection of qualified contractors compliant with the defined company procedure	Internal audit for checking the correct application of the selection procedure of qualified contractors and for assessing the contractor competence against the relevant qualification scheme. Check continuous contractor's compliance with the required qualification scheme trough inspections, Request the contractor through contractual arrangements to report the results of any internal or third party audit results and any other issue affecting the validity of the relevant certificate.
		2. Mandatory training for workers employed by the contractor.	The competence management system of the company is updated with a procedure to ensure that: (a) the company training program includes also training of the external staff which is performing safety tasks; (b) a final evaluation of that external staff knowledge is performed.	Monitoring of knowledge of contractor's workers is done through the final evaluation exam. Audit the correct application of the process. Use specific indicators to measure the efficiency of the training for the external workers. Direct supervision of the external workers by the railway company is foreseen in contractual arrangements.
The contractor is not conscious of the impact of its work on the safety level of the railway system	Service delivered by the contractor is not compliant with the technical and safety requirements Fatalities or (severe)	3. Inform the contractor in a documented way, supported by bilateral meetings, on possible consequences of contractor workers' mistakes and on the overall impact of its activities on the railway system	Contractor warned about impacts of its work on the safety of the railway system Communication on risks through bilateral meetings with contractor's workers	Check during internal audits that the contractor's workers were informed about the impacts of their work on the safety of the railway system Check also that bilateral meetings were done

Table 12: Example of FMEA for an outsourced activity.

Hazard	**Consequences**	**Safety requirement**	**Demonstration of compliance**	**Monitoring activity**
	injures of external workers	4. Mandatory training for workers employed by the contractor.	The competence management system of the company is updated with a procedure to ensure that: (a) the company training program includes also training of the external staff which is performing safety tasks; (b) a final evaluation of that external staff knowledge is performed	Monitoring of knowledge of contractor's workers is done through the final evaluation exam. Audit the correct application of the process. Use specific indicators to measure the efficiency of the training for the external workers. Direct supervision of the external workers by the railway company is foreseen in contractual arrangements.
The workers of the contractor are not aware of the hazards coming from the new working environment	Fatalities or (severe) injuries of external workers	5. Mandatory training for workers employed by the contractor.	Same as above	Same as above
The railway company produces instructions or contractual arrangements where there is room for interpretation	Contractor not aware of the contractual safety requirements. Contractor is not aware of its responsibilities.	6. Consultancy for contract definition	Consultancy contract established	No direct monitoring is foreseen for this action
		7. Contract management procedure foresees a continuous improvement of the contract	Procedure	Collection of feedback related to the issues arising from contract interpretation
…	…	…	…	…

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 15] Considering again Table 12, it can be seen that the safety requirements n° 2, 4 and 5 are related to the competences of external workers. The strategy of the railway company is to use its internal training process to mitigate the risks related to the activity of the contractor. It is possible to define, as examples, some indicators based on the company expertise only by analysing the training process.

[G 16] A possible basic structure of a training process is shown in Figure 6:

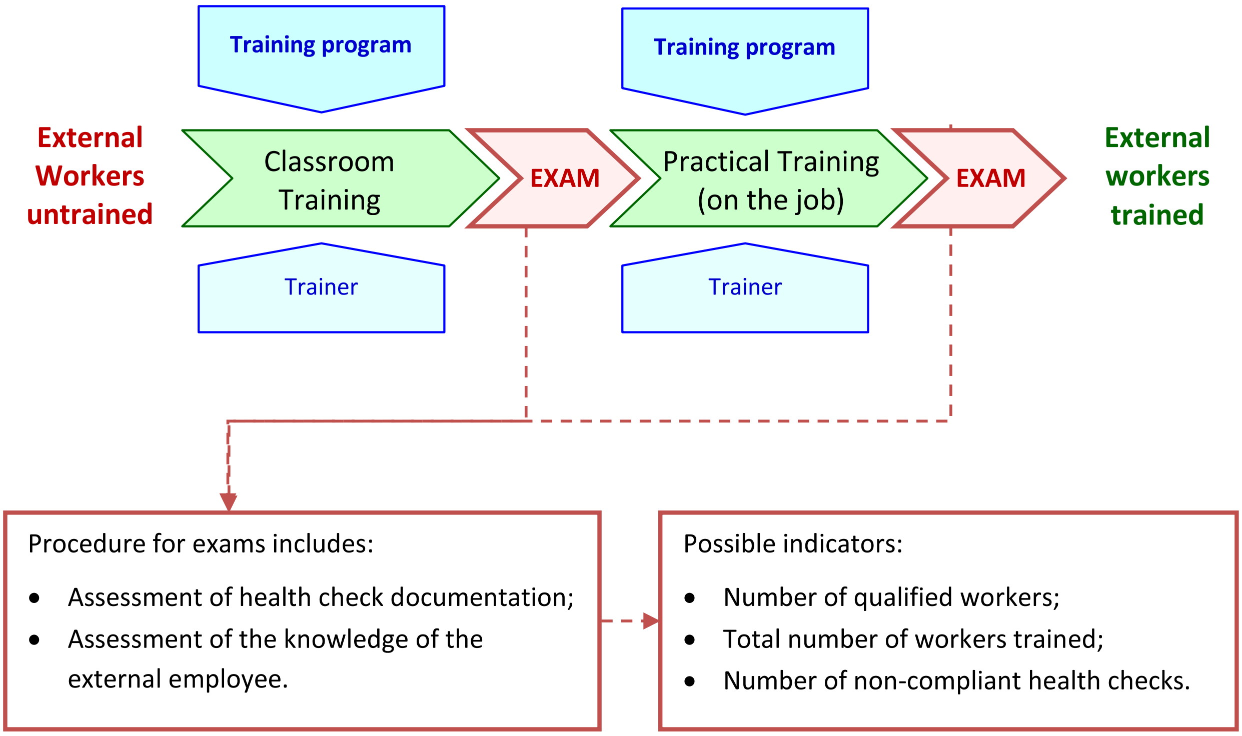


Figure 6: Possible basic structure of a training process.

Article 3 (2)

The monitoring process shall contain the following activities:

(a) the definition of a strategy, priorities and plan(s) for monitoring;

(b) the collection and analysis of information;

(c) the drawing up of an action plan for instances of unacceptable non-compliance with requirements laid down in the management system;

(d) the implementation of the action plan, if such a plan is drawn up;

(e) the evaluation of the effectiveness of action plan measures, if such a plan is drawn up.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] Guidance on the different steps of the monitoring process is available in the chapter "Explanations of the Annex in the Regulation on CSM for monitoring".

Article 4. Exchange of information between the involved actors

Article 4 (1)

Railway undertakings, infrastructure managers and entities in charge of maintenance, including their contractors, shall ensure through contractual arrangements that any relevant safety-related information resulting from applying the monitoring process set out in the Annex is exchanged between them, to enable the other party to take any necessary corrective actions to ensure continuous achievement of the safety performance of the railway system.

[G 1] Risks that are not sufficiently controlled may be identified during the monitoring activities by the railway undertakings, infrastructure managers and entities in charge of maintenance or their contractors.

[G 2] If the actor who detects the problem cannot take any corrective action, because the application of the related risk control measure is up to another railway actor, the CSM for monitoring requires this actor to inform the risk owner (as it should be defined in the contractual arrangements). The risk owner is then able to undertake or to manage the implementation of the necessary corrective actions.

[G 3] Nevertheless it can happen that the setup of the responsibilities, concerning the detected issue, is not the most efficient solution from the system-as-a-whole point of view. For example, the situation could have changed during the lifecycle of the railway system. Indeed, although the information about insufficiently controlled risks might be reported to another actor who is able to undertake corrective actions, it is possible that this actor (who does receive the information) is not any more the initial risk owner. In such a case, the setup of the responsibilities should be revised as well as the contractual arrangements that define it.

[G 4] In order to manage the situations described above, the CSM for monitoring requires that any need for exchanging safety related information is identified within the contracts between railway undertakings, infrastructure managers, entities in charge of maintenance and their contractors. If possible, before signing the contracts they should undertake a joint analysis of what kind of information they expect to exchange between them. The set of information to be exchanged can be defined through a similar risk assessment approach as illustrated in Article 3 (1) under the sub-title - More about "monitoring the contractors".

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Article 4 (2)

If, through the application of the monitoring process, railway undertakings, infrastructure managers and entities in charge of maintenance identify any relevant safety risk as regards defects and construction non-conformities or malfunctions of technical equipment, including those of structural sub-systems, they shall report those risks to the other parties involved to enable them to take any necessary corrective actions to ensure continuous achievement of the safety performance of the railway system.

[G 1] Usually the interfaces between the different railway stakeholders are well known beforehand. Consequently, any necessary exchange of safety related information, including the exchange of information about non-sufficiently controlled risks, is to be defined through contractual arrangements.

[G 2] Where a new risk is detected but there is no contractual arrangement in force, it is also important to appropriately address the risk and to undertake the necessary corrective actions. The traceability of decisions and of the allocation of responsibilities needs also to be granted.

> Systematic failures of technical equipment detected after the warranty period are a common example of risks controllable by another actor but where there is no more contract in force. The manufacturer is the best able actor to correct the failures in the most appropriate way. He has the full knowledge of the design of the technical equipment and also the visibility of all other users affected by those failures of the same technical equipment (or possibly of a reference system under the meaning of the CSM for risk assessment) which also need appropriate corrective measures.

[G 3] By virtue of Article 4(3) of Directive 2004/49/EC, the railway undertaking, infrastructure manager or entity in charge of maintenance who detects such systematic failures in its part of the system, including in the supply of material and contracting of services, is responsible for controlling the associated risks and thus for managing the correction of these failures. In that case, the railway undertaking, infrastructure manager or entity in charge of maintenance is free to decide either:

(a) to define and implement appropriate corrective measures by itself.

In this case, Article 4(2) of the CSM for monitoring requires the railway undertaking, infrastructure manager and entity in charge of maintenance to *"report those risks to the other parties involved to enable them to take any necessary corrective actions to ensure continuous achievement of the safety performance of the railway system"*. The purpose of this requirement is to enable the manufacturer to correct the same "defects and construction non-conformities or malfunctions of technical equipment" used by other actors, e.g. by other railway undertakings, infrastructure managers, entities in charge of maintenance or Member States.

or;

(b) to contract the definition and implementation of corrective actions to the manufacturer.

In this case, as the manufacturer has the full visibility of all other users affected by the same failures of the same technical equipment (or possibly of a reference system under the meaning of the CSM for risk assessment), he is able to undertake an appropriate action plan for correcting the problem for all users of the same technical equipment.

[G 4] Consequently, if any defects and non-conformities or malfunctions of technical equipment, in particular those of structural sub-systems, are detected, it is important to inform the right actor(s). Usually that would be the manufacturer which can then undertake an action plan to remedy the cause (preferably the root cause, however depth and effort of the analysis should be proportionate to the risk) and ensure a *"continuous achievement of the safety performance"* of the railway system as a whole.

[G 5] Note: When possible, a format or templates for exchanging safety related information (concerning defects and construction non-conformities or malfunctions of technical equipment) should be defined in advance. This enables targeted and proportionate information to be exchanged. For further elements on the importance of the configuration of safety information section 8.3.1 of {Ref. 3} can be consulted.

[G 6] So, in addition to correcting systematic failures within their areas of responsibility, as far as known by railway undertakings, infrastructure managers and entities in charge of maintenance, *"they shall"* also *"report"* the detected *"risks to the other"* right *"parties involved to enable them to take any necessary corrective actions"* within their areas of responsibility *"to ensure continuous achievement of the safety performance of the railway system"* as a whole. Nevertheless, it is possible that the actor who discovers defects and non-conformities or malfunctions of technical equipment does not know who is able to define and implement the most appropriate action plan (e.g. bankruptcy of the manufacturer). In such cases, the actor may consult the national safety authority of the Member State where the defects, non-conformities or malfunctions are discovered. Based on this information, the national safety authority can help the actor to find out which other actor or company is the best placed for solving the problem. However, as explained in Article 4 (2)[G 3], informing the national safety authority does not remove the obligation of the railway undertaking, infrastructure manager or entity in charge of maintenance to control the risks of the part of the railway system which falls under its responsibility.

[G 7] It is also important to note that the national safety authority cannot be used as a systematic way for reporting identified problems and transferring to them the responsibility of finding out who is the right actor(s) for implementing the corrective measures at the level of the European railway system. Although the national safety authority can be put in copy of the exchanges of safety related information, railway undertakings, infrastructure managers and entities in charge of maintenance are expected to find out themselves the solution with the initial manufacturers of the concerned technical equipment.

Article 5. Reporting

Article 5 (1)

The infrastructure managers and railway undertakings shall report to the national safety authority on the application of this Regulation through their annual safety reports in accordance with Article 9(4) of Directive 2004/49/EC.

[G 1] In the scope of the reporting to the national safety authority on the effectiveness of their safety management system, it is necessary to include also the experience of the railway sector with the application of the CSM for monitoring. The purpose is to allow the European Railway Agency to evaluate its applicability and effectiveness. Both positive and/or negative feedbacks concerning the implementation of the mentioned CSM are expected.

Article 5 (2)

The national safety authority shall report on the application of this Regulation by the railway undertakings, infrastructure managers, and as far as aware of it, by the entities in charge of maintenance in accordance with Article 18 of Directive 2004/49/EC.

[G 1] Similarly, in the scope of the reporting to the European Railway Agency on the safety regulation, supervision and performance in their Member State, it is necessary that the national safety authority includes also the feedbacks from their stakeholders with the application of the CSM for monitoring.

[G 2] In case the certification of entities in charge of maintenance is carried out and surveyed by the national safety authority, they can also include in their annual safety report the feedbacks on the CSM for monitoring from those entities in charge of maintenance.

[G 3] The benefit is to get a synthesized view of the experience of the railway stakeholders in the considered Member State. The overall purpose of the reporting is to allow the European Railway Agency to evaluate the applicability and effectiveness of the CSM for monitoring.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Article 5 (3)

The annual maintenance report of entities in charge of maintenance of freight wagons set out in point I.7.4(k) of Annex III to Regulation (EU) No 445/2011, shall include information about the experience of entities in charge of maintenance in applying this Regulation. The Agency shall gather this information in coordination with the respective certification bodies.

[G 1] Similarly, in the scope of the annual maintenance reporting to the ECM certification body on the effectiveness of their system of maintenance, it is necessary that the entities in charge of maintenance include also their experience with the application of the CSM for monitoring.

[G 2] This annual maintenance report is intended for the ECM certification body to enable it to target its surveillance activity.

[G 3] The European Railway Agency should gather this information in coordination with the respective ECM certification bodies to enable it to evaluate the applicability and effectiveness of these actions in the field of rolling stock maintenance.

Article 5 (4)

The other entities in charge of maintenance that do not fall under the scope of Regulation (EU) No 445/2011 shall also share their experience with the Agency on the application of this Regulation. The Agency shall coordinate the sharing of experience with these entities in charge of maintenance.

[G 1] Entities in charge of maintenance not involved with the rolling stock included in the scope of the Regulation (EU) No 445/2011 are also requested to provide their feedback to the European Railway Agency on their experience with the application of the CSM for monitoring.

[G 2] However, as those entities in charge of maintenance are not legally required to produce an annual maintenance report, the CSM for monitoring does not oblige them either. In order to enable the European Railway Agency to evaluate the applicability and the effectiveness of the CSM for monitoring, in the field of maintenance of other rolling stock than freight wagons, the Agency will coordinate with such entities in charge of maintenance to share their experience.

Article 5 (5)

The Agency shall collect all information on the experience of the application of this Regulation and, when necessary, shall make recommendations to the Commission with a view to improving this Regulation.

[G 1] As explained in Article 5 (1), Article 5 (2), Article 5 (3) and Article 5 (4) above, the European Railway Agency collects from many sources the experience of the railway sector with the application of the CSM for monitoring.

[G 2] The Agency's role in relation to this matter is to analyse the collected information and identify the difficulties encountered by the different actors who are applying the CSM for monitoring. The purpose is to evaluate the applicability and the effectiveness of the CSM in itself and to propose to the European Commission improvements of the method based on the feedback and challenges encountered during the application of this CSM.

Article 5 (6)

The national safety authorities shall support the Agency in collecting such information from railway undertakings and infrastructure managers.

[G 1] Within this context, the national safety authorities can help the European Railway Agency to better target the stakeholders who have sufficient and relevant experience in the application of the CSM for monitoring.

[G 2] Through their supervision role of the safety management system, or surveillance role of the system of maintenance for the national safety authorities who act also as ECM certification body, the national safety authority has the best picture of the railway sector experience in his Member State. The national safety authority knows at best which actor or company faced a difficulty with the application of the method.

[G 3] Based on this information, the Agency can then enter into contact with those actors and share with those actors/companies the difficulties they face.

Article 5 (7)

The Agency shall submit to the Commission not later than three years after the entry into force of this Regulation a report analysing the effectiveness of the method and of the experience of railway undertakings, infrastructure managers and entities in charge of maintenance in applying this Regulation.

[G 1] No explanation needed.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Article 6. Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
This Regulation shall apply from 7 June 2013.

[G 1] No explanation needed.

EXPLANATION OF THE ANNEX IN THE REGULATION ON THE MONITORING PROCESS

1. General

1.1. The inputs to the monitoring process shall be all the processes and procedures contained in the management system, including the technical, operational and organisational risk control measures.

1.2. The activities referred in Article 3 (2) of the monitoring process are described in Sections 2 to 6.

1.3. This monitoring process is repetitive and iterative, as shown in the diagram below in the Appendix.

[G 1] The monitoring process is an iterative process of the management system: see (Figure 8). It enables to verify if the application of the management system is correct and if the expected outcomes, including the company safety targets, are met. If not, the monitoring process requires to take corrective and/or preventive measures and, in the next cycle of the monitoring activities, to verify if these new measures bring the proposed improvements or if further new measures need to be considered.

[G 2] As any other process of the management system, the monitoring process is composed of the same 5 essential components (see Figure 7): the process itself, the procedures to be applied, resources who are going to apply the process and procedures, inputs and outputs.

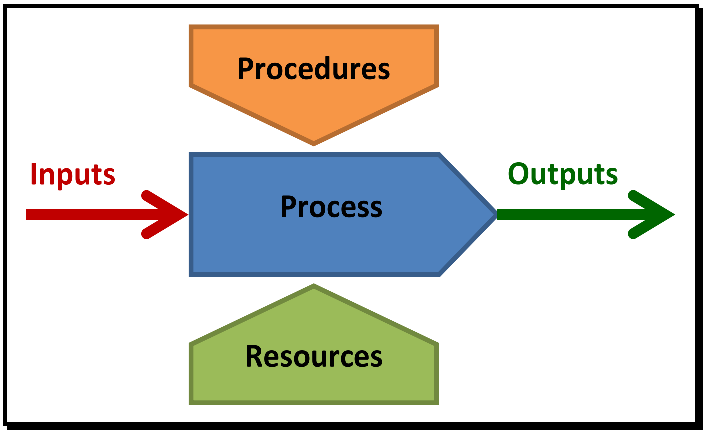


Figure 7: Generic representation of a process, applicable also to the monitoring process.

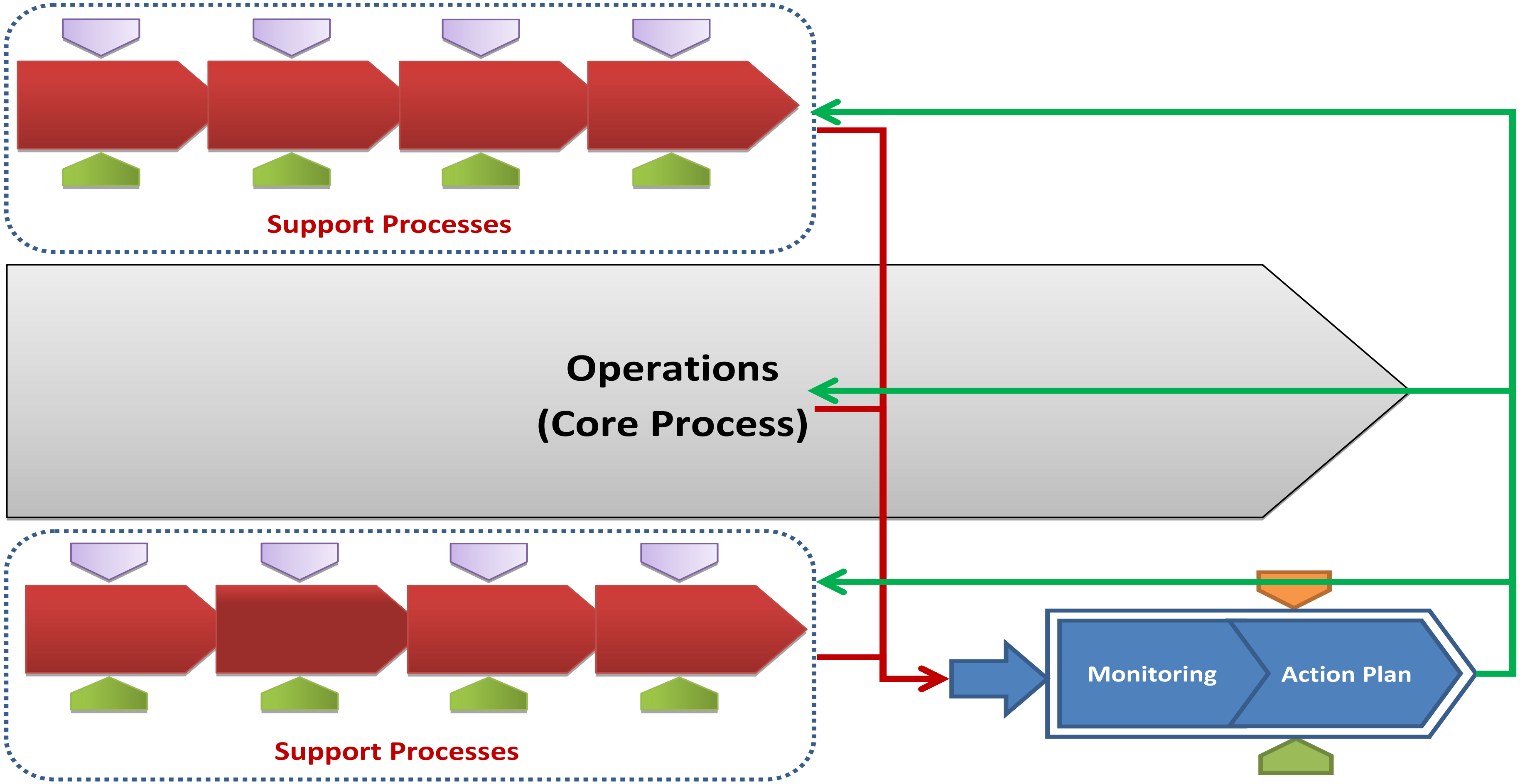


Figure 8: Example of the structure of a management system.

[G 3] The legal text clearly states that all the processes and procedures of the management system must be monitored. Nevertheless, freedom is given to the user to prioritise its monitoring activities according to the specific needs of the company. It is thus important to define clearly in the management system the criteria for this prioritisation. For instance these criteria can be based on the results of a risk assessment activity or on expert judgement.

Why is monitoring necessary?

[G 4] In order to control the risks that can arise from a specific activity:

(a) predictive risk control measures (*they can be of technical, organisational or operational nature*) are defined and implemented;

(b) the correct application and the effectiveness of those predictive risk control measures need to be verified (i.e. monitored) in practice to ensure that the assumptions made during the risk assessment remain valid;

(c) the importance of monitoring risk control measures is that the user needs to be aware that the predictive risk control measure, e.g. a technical system *(respectively an operational procedure)*, is one side providing a sufficient level of protection, and on the other side that it has not failed *(respectively it is continually correctly applied)*. If this is not achieved, the considered risk is no more under control, or at least the acceptability of the risk can be compromised.

[G 5] In this view, the monitoring process can be considered itself as an additional safety requirement because it is functioning as a proactive risk control measure. In case the monitored risk control measure fails, the user is informed by the monitoring activity that the expected level of protection is not met. The railway system works in a degraded mode and the associated risk is no more controlled due to the failure of the monitored risk control measure.

[G 6] The following example illustrates the concepts described in sections [G 3] and [G 4] above on the monitoring of the effectiveness of risk control measures.

Example 3:

In order to prevent train derailments caused by an overspeed above the permitted speed limits, the railway undertaking decides to supervise the driver by an on-board Automatic Train Protection (ATP) equipment. When the ATP fails, the ATP provides the driver with a failure indication on the speed indication display.

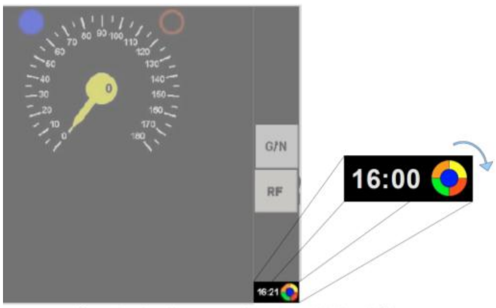


Figure 9: Speed indication in ATP.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 7] Table 13 gives an extract of the risk assessment done for the overspeed hazard and the selected risk control measure (i.e. the use of an ATP). The table also shows the information that should be monitored to check the effectiveness of the risk control measure (i.e. of the ATP).

Table 13: Identification of information to monitor concerning failures of an ATP.

Hazard	Consequences	Safety Requirement	....	Monitoring activity
Overspeed	Train derailment	• Use a technical system (e.g. ATP) for supervising the train speed against the maximum permitted speed limit • Use of ATP to display the train speed	...	• The technical system shall include a self-monitoring function to inform the operational staff (i.e. the train preparer or the train driver) about its safe working status. • The train driver shall log the malfunctioning of the ATP in the locomotive book. • The ECM shall communicate to the keeper the critical faults detected during the maintenance of the technical system.

[G 8] As the ATP is used on one side to display the train speed, and on the other side to prevent the driver from exceeding the permitted speed limitation, it is important that the driver is aware about failures of the ATP. The ATP indicates the train speed on a Driver Machine Interface (DMI) display: see Figure 9. To ensure that the speed indication is continuously refreshed, a small icon is placed in the bottom-right corner of the display. When the ATP is fully working, the icon rotates, meaning that the ATP is not dead and that the DMI is fully working (i.e. it indicates the right speed and the ATP supervises the driver). This icon can be considered as a measure that is part of a monitoring interaction in the "driver-ATP" system. The icon is an internal function of the ATP. It can be considered as a risk control measure.

How to identify what is to be monitored?

[G 9] In order to ensure that the safety targets of the railway system are met and that the safety level does not gradually degrade during the operation and maintenance, all the safety-related activities of the company, and consequently all the processes and procedures of the management system, including the technical, operational and organisational risk control measures are to be monitored.

[G 10] It is important to mention that other requirements for monitoring than those linked to the management system of the company can result from the implementation of TSIs, national rules, use of external safety documentation concerning technical systems (e.g. instructions, maintenance files, etc.).

[G 11] The users can identify what is necessary to be monitored using a "process mapping technique" on their management system.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 12] A summary of the inputs to consider for the definition of what is necessary to be monitored is represented in Figure 10.

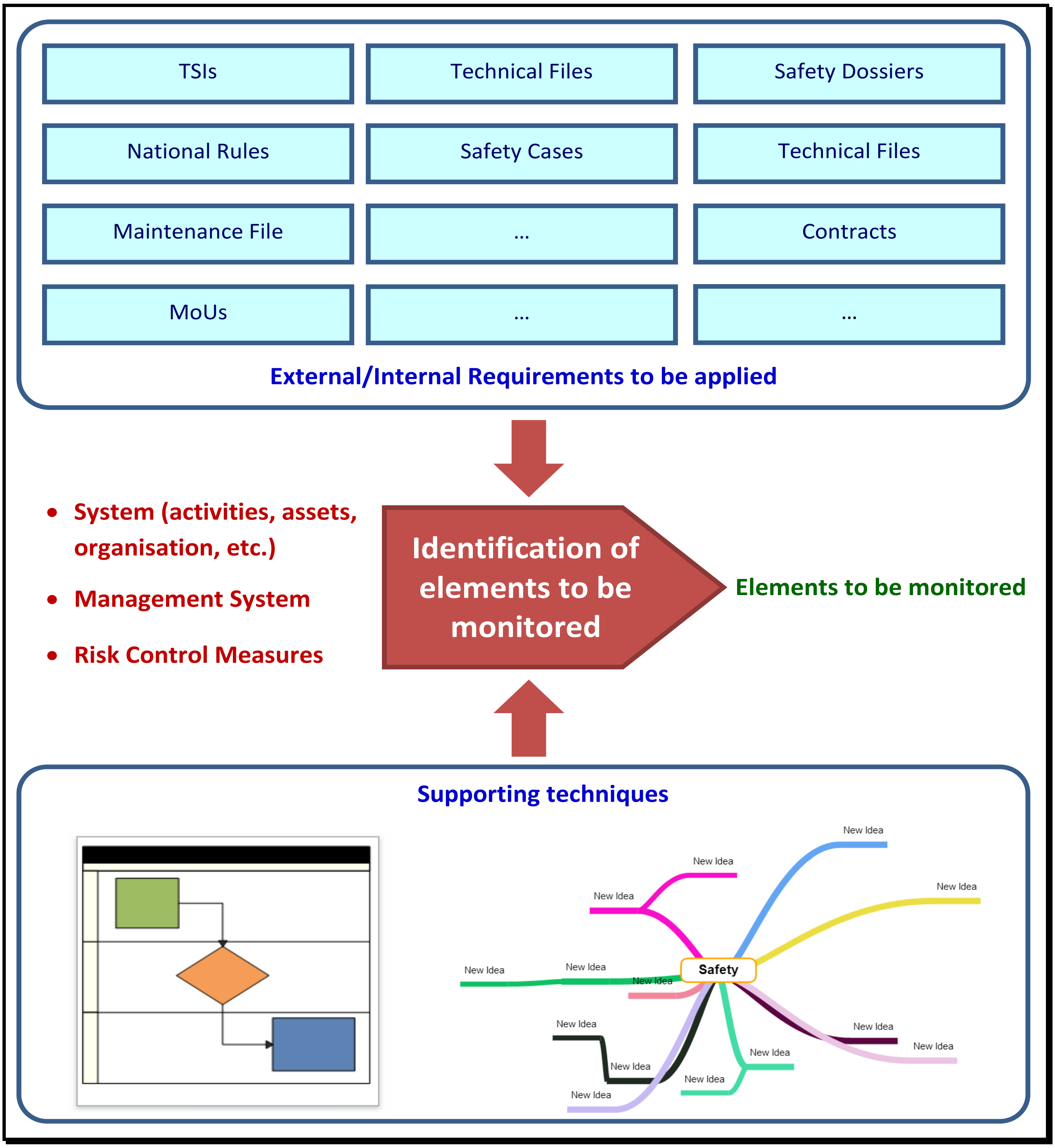


Figure 10: Identification of the elements to be monitored.

[G 13] For designing and prioritising the monitoring activities specific to the company, it is necessary to have a sufficiently detailed picture of:

(a) What risks the operation gives rise to?
(b) What risk control measures are implemented to control those risks?

[G 14] The knowledge of this information is crucial for identifying what to measure/check/etc. (i.e. what to monitor?) to be able to detect on time any deterioration of the processes, procedures or other non-compliances which could affect the safety level and lead to a non-acceptable level of risk.

[G 15] A typical document supporting this step is the Hazard Record, also known as Hazard Log, that is produced during the risk assessment activities.

2. Definition of a strategy, priorities and plan(s) for monitoring

2.1. *Based on their management system, each railway undertaking, infrastructure manager and entity in charge of maintenance shall be responsible for defining its strategy, priorities and plan(s) for monitoring.*

2.2. *The decision on what to prioritise shall take into account information from areas that give rise to the greatest risks and, if not monitored effectively, could lead to adverse consequences for safety. An order of priority for monitoring activities shall be set, and the time, effort and resources required shall be indicated. Prioritisation shall also take into account results from previous applications of the monitoring process.*

2.3. *The monitoring process shall identify as early as possible instances of non-compliance in the application of the management system that might result in accidents, incidents, near-misses or other dangerous occurrences. It shall lead to the implementation of measures to remedy such instances of non-compliance.*

2.4. *The monitoring strategy and plan(s) shall define either quantitative or qualitative indicators or a mixture of both that can:*

(a) *give early warnings of any deviation from the expected outcome, or assurance that the expected outcome is achieved as planned;*

(b) *give information about unwanted outcomes;*

(c) *support decision making.*

Defining a strategy for monitoring

[G 1] The term "strategy" can have different meanings according to the context in which these words are used. A strategy, in the context of monitoring, can be defined as a high-level plan to achieve a goal. A strategy is needed because, to achieve the goal, a limited budget and number of resources are available. They need to be used in the most efficient way by providing the criteria to prioritise the monitoring activities.

[G 2] Considering the above mentioned definition of strategy for monitoring, there are at least two key elements to be explained in order to allow the user to establish its own monitoring strategy. It can be stated that monitoring a management system has the aim to provide useful elements for checking on one side that the safety targets are met, and on the other side for improving the management system. Moreover, the legal text prescribes a proactive approach in order to get early-warnings concerning a possible occurrence of accidents, incidents, near-misses or other dangerous occurrences:

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) a **Railway Undertaking** or an **Infrastructure Manager** needs the outcomes of the monitoring process to prevent the occurrence of accidents, incidents and other unwanted events, improving in this way the safety management system;

(b) an **Entity in Charge of Maintenance** needs the outcomes of the monitoring process to prevent systematic and random mistakes, in the maintenance process, that can compromise the technical characteristics of the rolling stock and its safety level while being operating, improving in this way the system of maintenance.

[G 3] The strategy should include also the main organisational structure of the monitoring:

(a) in big companies it could be necessary to allow low-mid managers to continuously adjust the monitoring process, e.g. defining a new indicator or a new procedure to collect data or, according to their responsibility, a new procedure for data analysis;

(b) vice versa, in small companies, the management of the monitoring process can be centralised allowing operational staff and managers to propose changes to be analysed and implemented by the person identified as process owner.

The management system should be structured to allow the setup of the monitoring process, giving the necessary independence to the peripheral structures and establishing the adequate responsibilities.

[G 4] A monitoring strategy and plan(s) could, among others, include a description of the following (more explanations on every point in the list follow after the list):

(a) external/internal requirements to be applied: e.g. CSM for monitoring, CSM for risk assessment, TSIs, national rules, etc.;

(b) specific needs of the company (business aspects can be included);

(c) definition of criteria for prioritisation of monitoring;

(d) criteria to link timing for monitoring with the characteristics of the activity to be monitored;

(e) responsibilities in monitoring, including the organisational structure of the monitoring process;

(f) monitor techniques.

[G 5] The strategy should define, at least in a general way, the approach to be followed in the definition of safety targets.

[G 6] The strategy should define, at least in a general way, which organisational and technical tools will be used for gathering monitoring information within the company. A set of common data collection tools can be the following:

(a) pre-designed intervals on certain indicators;
(b) inspections, interviews;
(c) hierarchical checks;

(d) audits (refer to ISO 19011 for further information);
(e) accident, incident and near misses reporting and investigations;
(f) fault reporting;
(g) informal channels, e.g. staff feedback, customer feedback, etc.

Several of these methods can be used or combined within the same company or organisational structure.

[G 7] The strategy should also define the principles for the analysis of the gathered data. For example, it can be clarified if the analysis is done in a specific and centralised organisational structure or if each of the structures of the company is responsible for the analysis of its own data. The strategy could also include the techniques for the data analysis, for example:

(a) statistical data analysis;
(b) expert judgments;
(c) brainstorming sessions;
(d) others.

[G 8] The strategy can be formalised in a specific document (e.g. Safety Policy or Safety Manual) or it can be shared among the documents of the SMS (e.g. high level procedures).

How to prioritise the monitoring activities

[G 9] The CSM states that *"all the processes and the procedures of the management system shall be the input of the monitoring process"*. However, the CSM for monitoring also allows the prioritisation of the monitoring activities.

[G 10] It means that all the processes are to be monitored, but the frequency and the detail of the monitoring activity can be different from a process to another one and dependent on the specificity of every company.

[G 11] Prioritisation is a mean for improving the efficiency of the monitoring process, which shall cover the whole management system, focusing in particular on the most risky activities and *"areas that give rise to the greatest risks and, if not monitored effectively, could lead to adverse consequences for safety"*.

[G 12] The organisation has, from the management system, knowledge about the greatest risks and the associated risk control measures. **The principle of prioritising is based on the level of risk.** This means that the processes, procedures and risk control measures do not necessarily need to be monitored with the same frequency and/or with the same intensity. Therefore priorities would need to be defined.

[G 13] The criteria driving the prioritisation are the risks associated with the specific activity of the company. In the framework of risk assessment a Risk Priority Number

(RPN=frequency * severity) can be defined to establish a priority for the definition of risk control measures and the associated monitoring requirements.

Table 14: Example of setting Risk Priority Numbers.

ID	Hazard	Risks	Classification	RPN
6	Shunting operation not authorized	Collision	Tolerable	0,75
7	Wrong path during shunting operation	Collision	Tolerable	0,60
33	Irregular shunting operation	Derailment	Acceptable	0,12

[G 14] The three hazards listed as example in Table 14 have been identified by a company which is interested in changing its shunting procedures. The procedure for assessing risks states that hazards can be classified as: Acceptable, Tolerable and Not Acceptable. This is a first criterion for prioritisation because tolerable risks are more dangerous than acceptable risks. Moreover, to prioritise the mitigation of risks belonging to the same acceptance category, an RPN is foreseen. From the table above, Hazard 6 has priority in mitigation and monitoring on Hazard 7.

[G 15] Considering the three levels of classification and the RPN, spacing from 0 to 1, a priority chart can be defined.

Table 15: Example of chart for the Risk Priority Numbers [RPN=f*S]..

		0 --------------------->Risk Priority Number----------------->1		
Classification	**Acceptable**			
	Tolerable			
	Not Acceptable			
	Low Priority		**Mid Priority**	**High Priority**

[G 16] High priority means essentially stricter control for monitoring a specific activity of the management system. The resources can be used, for example, to increase the frequency of inspections or audits, or to have a more detailed set of indicators describing the process. In case an unwanted event occurs and the number of indicators linked to it is not sufficient to identify the causes, the consequent investigation could be more demanding. This aspect should be taken into account in the allocation of resources.

[G 17] The frequency of monitoring should also be defined according to:

(a) experts' judgment;
(b) past implementation of monitoring;
(c) timing of the activity (a daily performed activity will require a higher monitoring frequency than a monthly performed one);
(d) other elements, in accordance with the management system of the company.

Planning the monitoring

[G 18] Planning of monitoring activities should be a consequence of the strategy and the criteria for prioritisation. In the section above describing the "strategy for monitoring", it is explained how the activity should be undertaken and the priorities should lead to an efficient allocation of resources.

[G 19] The planning step can be seen as the preparation for the executive steps. It should include the scheduling of all the activities related to monitoring, for example (the list is not to be considered as exhaustive):

(a) activities designed to collect data: audits, hierarchical checks, inspections, meetings with contractors, etc.;
(b) data analysis with operational staff or with the management;
(c) safety meetings for discussion of the safety performances with operational staff, front-line staff and (top) management or management at the appropriate level, depending on the specific structural organisation of the company;
(d) meetings for design and approval of the action plan;
(e) others.

Definition of indicators and safety targets

[G 20] In order to monitor all processes, procedures and risk control measures, it is possible to design appropriate indicators that can, when data is collected, give a picture of the effectiveness of more than one process, procedure or risk control measure. Therefore, measuring those well-chosen indicators at the frequency defined in accordance with the level of priority will provide an indication about the effectiveness and the correct application of all the associated processes, procedures and risk control measures.

[G 21] Depending on the specificities of every company, the indicators can be either quantitative (if possible) or qualitative or even a mixture of both. The company is free to decide on how to measure the compliance with the expected outcome of their management system. The qualitative indicators are very useful in the maintenance/safety policy or to monitor the trends of some type of dangerous events. For example in case of Signals Passed At Danger (SPADs) it can be preferable to act when the trend is showing an increase in the number of occurrences than waiting for overpassing the safety target.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 22] In general indicators need to be chosen carefully. It is necessary to consider the goal of the monitoring process and of the management system as a whole: avoiding accidents, incidents, near-misses or other dangerous occurrences. To achieve the goal, the indicators need to provide the necessary data (early warnings) to drive the decisions of the management towards the absence of unwanted events (accidents, incidents, near misses, non-conformities in maintenance, etc.). This type of indicators are named leading indicators[(7)] (also known as precursors).

[G 23] The role of indicators is also to provide a measure of the safety performances, to check if what has been implemented has been effective or not. Normally these indicators are associated to the occurrence of unwanted events such as accidents, incidents, near misses, non-compliances, etc. As they report on an unsuccessful control of risks (i.e. on unwanted events that already happened), these types of indicators are named lagging indicators[(8)].

[G 24] The definition of indicators is related also to the definition of associated safety targets. So, to check the correct application or the effectiveness of specific processes, threshold values can be setup for the associated quantitative indicators. For instance, considering the check of the effectiveness of the *"training process of train drivers"*, amongst others the indicator: *"number of train driver candidates rejected at the exam"* can be used.

Table 16: Example of definition of an indicator and the associated safety target.

Indicator	**Process to monitor**	**Safety Target**	**...**
...	...	...	...
Number of train driver candidates rejected at the exam	Competence Management System	20% of the candidates	...
...	...	...	...

[G 25] Table 16 shows that once the indicator is defined, an associated safety target should be set up to monitor whether the number of reported events linked to the indicator is acceptable or not. This concept of thresholds can be applied both to leading and lagging types of quantitative indicators.

[G 26] A list of leading and lagging indicators is provided in the Annex I of the safety Directive 2004/49/EC.

(7) *Leading indicators are also known in other literature as "proactive indicators".*

(8) *Lagging indicators are also known in other literature as "reactive indicators".*

[G 27] The ability to define leading indicators is linked to either the experience, as a result of previous investigations of accidents, incidents or in general of unwanted events, or other sources such as the company knowledge of the chain of events that can drive to an accident (e.g. from risk evaluation and assessment). The chain of events that can lead to an unwanted event (causes/precursors) can be determined with the use of some techniques such as a Fault Tree Analysis. An example of a Fault Tree Analysis is shown in Figure 11.

[G 28] The identification of the right indicators enables to collect the appropriate monitoring data and information in a systematic way. Then the collected monitoring data and information can be analysed to either have an indication on whether something starts becoming a problem (data on leading indicators) or to find out the safety outcome in terms of actual safety performance (lagging indicators).

[G 29] Leading and lagging indicators need to be used in combination.

[G 30] According to Directive 2009/149/EC, amending the Directive 2004/49/EC, mandatory indicators are required (so called CSI, Common Safety Indicators). Examples of common safety indicators are, number of accidents (lagging indicators), number of broken rails and Signal Passed at Danger (SPAD) (leading indicators). The CSIs are collected at a Member State level and the data contribution from one company is therefore only a fraction of the sum for that Member State.

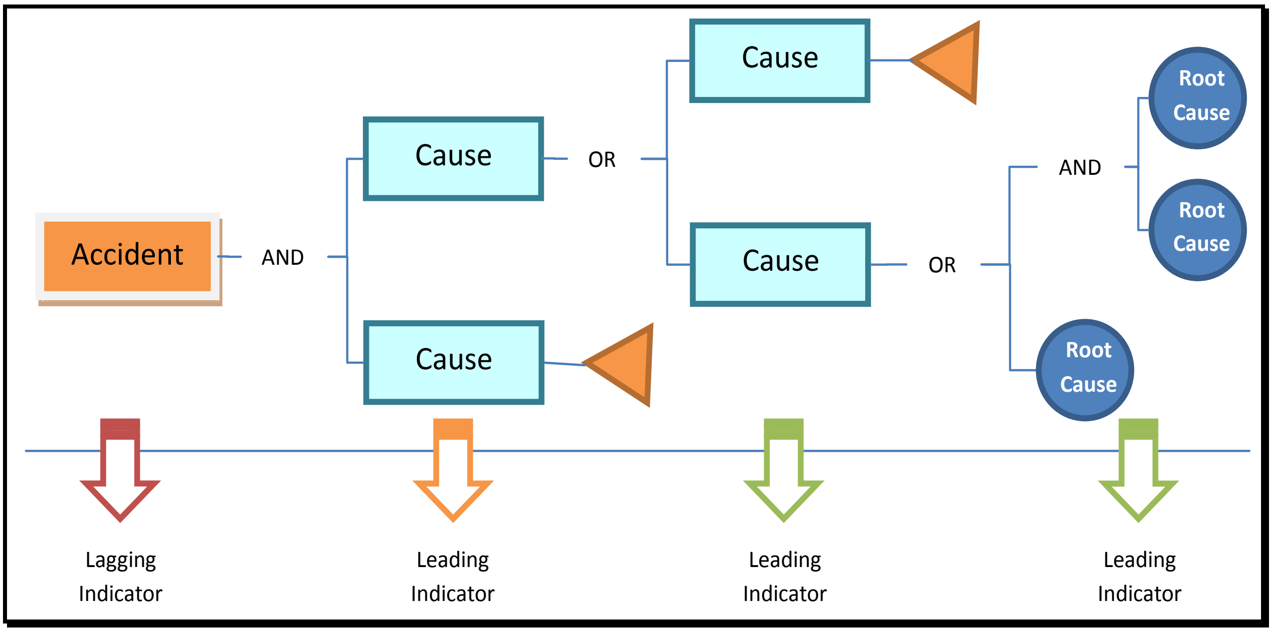


Figure 11: Example of a Fault Tree Analysis of the causes leading to an accident.

[G 31] In some countries, the national legislation may prescribe the use and reporting of some mandatory national indicators. By virtue of Directive 2004/49/EC, those national requirements are reflected within the company management system and associated indicators are taken into account within the monitoring process.

[G 32] All indicators need to have a "unit of measurement", for which the data is collected. The indicators need to be chosen in order to reveal any weaknesses of the processes and procedures contained in the management system, including of any risk control measures.

[G 33] All indicators need also to be accompanied by a proper definition. See from page 64 of this document the illustrative examples of monitoring activities.

[G 34] Indicators that support the data analysis should be defined. For example, it is of less use to analyse the number of signals passed at danger (SPADs) without considering the actual traffic volume (please refer to Figure 5 as example).

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

3. Collection and analysis of information

3.1. The collection and analysis of information shall be carried out according to the strategy, priorities and plan(s) defined for the monitoring.

3.2. For each defined indicator referred to in point 2.4, the following shall be carried out:

(a) a collection of necessary information;

(b) an evaluation as to whether the processes, procedures, technical, operational and organisational risk control measures are correctly implemented;

(c) a check on whether the processes, procedures, technical, operational and organisational risk control measures are effective and whether they achieve the expected outcomes;

(d) an evaluation of whether the management system as a whole is correctly applied and whether it achieves the expected outcomes;

(e) an analysis and evaluation of instances of identified non-compliance with points (b), (c) and (d), as well as identification of their causes.

Collection of information

[G 1] The collection of data should be done in accordance with the procedures of the management system. The procedures should grant the reliability of the data; for example ensuring that duplication of data is avoided.

[G 2] The management system should include the description of the organisational tools used to collect data. The tools should be defined in the strategy, as described in Chapter 2, paragraph [G 6].

[G 3] The management system should contain instructions for using and maintaining technical tools for monitoring, such as IT tools, on-board recording devices, etc. For instance, in case data are stored in a database, rules, procedures and responsibilities shall be defined to ensure reliability of data and traceability of the data input; a policy to access and share data is necessary to avoid misuse of information from unauthorised personnel.

Analysis of information: format and quantity of data to be analysed

[G 4] Data analysis is not a single step activity. According to the safety policy of the company and the strategy for monitoring, the line management could be able (or might need) to analyse data in order to proceed to a self-assessment. A further analysis can be performed by the safety experts to assess the overall safety performance of the company. The final analysis can be done by the top management, for instance to define an appropriate budget for safety or to approve an action plan designed to improve the safety level of the company.

[G 5] The top management, the line management and the safety experts probably need different quantity of information with a different level of detail. It can be opportune to predefine, in the management system, a standard setup for information for each of the analyses that will be undertaken. This step is important to facilitate the comprehension of the safety information.

Analysis of information: criteria for data analysis and safety targets

[G 6] The criteria, roles and responsibilities for the evaluation should be described in the management system.

[G 7] The criteria for the evaluation of the effectiveness and of the correct application of the management system need to be linked with the safety targets.

[G 8] Safety targets need to be defined starting from the safety/maintenance policy. The policy can use qualitative safety targets to address the organisation in developing actions, which can lead to a reduction of unwanted events.

[G 9] Comparisons are carried out between "the design of how to use the processes, procedures, technical, operational and organisational risk control measures" and the outcome of their application. Observing Figure 12 as consequence of the results of the monitoring activity the system has been modified to measure the improvement of the following two safety targets:

(a) a qualitative one, concerning the trend of the unwanted event: Reduction of SPAD;

(b) a quantitative one, concerning a threshold for the specific indicator: 4 SPADs/million train*km

In this specific case, the first step of the data analysis could consist in comparing the value reported for the indicator with the quantitative safety target set up for the indicator.

[G 10] Comparisons should be also carried out between the expected level of safety and the one actually delivered by the management system. This is crucial to make an evaluation of the effectiveness and of the implementation of the system as a whole.

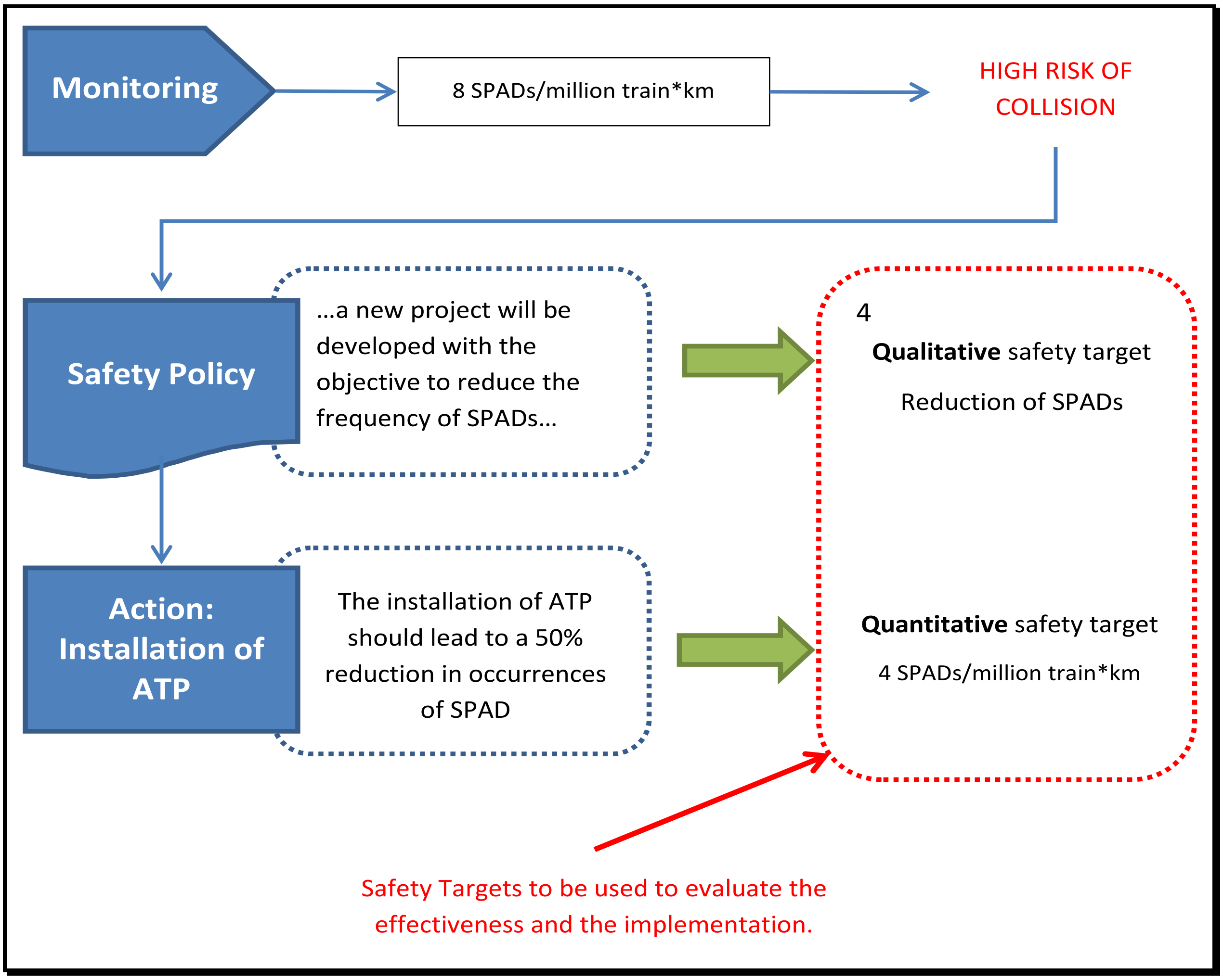


Figure 12: Example of definition of safety targets.

4. Drawing up of an action plan

4.1. For identified instances of non-compliance that are considered unacceptable, an action plan shall be drawn up. This shall:

(a) lead to the enforcement of correctly implemented processes, procedures, technical, operational and organisational risk control measures as specified, or;

(b) improve existing processes, procedures, technical, operational and organisational risk control measures, or;

(c) identify and implement additional risk control measures.

[G 1] As described in guidance of section 4.2, the purpose of the action plan is to decide on what measures need to be taken if it is judged necessary to restore the degraded safety margins, to improve the safety or to improve the management system. The first step here is to decide if any action is needed or whether the level of non-compliance found is tolerable.

[G 2] As explained in previous sections, the monitoring strategy may tolerate non-compliances with respect to specified requirements. Non-compliances can be acceptable as long as designed thresholds/tolerance levels for the associated indicators are not reached. Consequently, immediate implementation of corrective/preventive measures is not always necessary. The strategy should describe any mechanisms by which non compliances are reviewed and deemed tolerable.

[G 3] On the contrary, if the non-compliance is judged to be non-acceptable, the action plan needs to include what to do: see annex section 4.2.

[G 4] The management, at the appropriate level of the company structural organisation, is finally responsible to decide about the need and the implementation of an action plan, unless the action plan is requested by applicable legislation or other legal provisions.

[G 5] The management, at the appropriate level of the company structural organisation, is responsible to approve the project and to provide adequate resources for its development, implementation and future evaluation of its effectiveness.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

4.2. The action plan shall in particular include the following information:

(a) objectives and results expected;
(b) corrective, preventive or both type of measures required;
(c) person responsible for implementing actions;
(d) dates by which actions are to be implemented;
(e) person responsible for evaluating the effectiveness of the action plan measures in accordance with Section 6;
(f) a review of the impact of the action plan on the monitoring strategy, priorities and plan(s).

[G 1] The action plan should be developed according to the change management process of the management system. The final documentation should include the information requested by the CSM for monitoring and by the management system of the company.

[G 2] To be able in later stages to verify if the correct measure is taken, it is necessary to predict what a measure should lead to. This would typically include the expected safety outcome of the measure when it is implemented.

[G 3] The action plan includes all the details which are necessary to carry out the implementation of any new measures, changes in risk control measures, etc. The action plan needs to be detailed enough in order to be clear what is necessary to carry out and who and when the implementation must be finished. It also includes pointing out the responsibility in the next iteration to check if the actions meet the predicted expectations.

4.3. For managing safety at interfaces the railway undertaking, infrastructure manager or entity in charge of maintenance shall decide, with agreement of the other actors involved, who shall be in charge of implementing the required action plan or parts of it

[G 1] No explanation needed

5. Implementation on the action plan

5.1. The action plan defined in Section 4 shall be implemented so as to correct identified instances of non-compliance.

[G 1] The implementation of the action plan should be monitored in accordance with the procedures of the management system of the company and with the responsibilities assigned for the implementation of the action plan.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

6. Evaluation of the effectiveness of the action plan measures

> *6.1. Correct implementation, appropriateness and effectiveness of measures identified in the action plan shall be checked using the same monitoring process as described in this Annex.*
>
> *6.2. Evaluation of the action plan's effectiveness shall in particular include the following actions:*
>
> *(a) verification of whether the action plan is correctly implemented and completed according to schedule;*
>
> *(b) verification of whether the expected outcome is achieved;*
>
> *(c) verification of whether in the meantime the initial conditions have changed and the risk control measures defined in the action plan are still appropriate for the given circumstances;*
>
> *(d) verification of whether other risk control measures are necessary.*

[G 1] Section 6 of the Annex of the CSM for monitoring (i.e. the current section) essentially describes the concept of continuous improvement.

[G 2] After the detection of an issue in the outcomes of the management system processes or of the management system as a whole, an action plan, approved and supported by the management, at the appropriate level of the company organisational structure, needs to be adopted.

[G 3] The action plan needs to be designed in order:

(a) to achieve predefined safety targets;
(b) to be applicable to the company and to its operations;
(c) to enable the defined risk control measures to be monitored.

[G 4] After the implementation of the action plan, an assessment of its results is necessary to verify that it delivers the expected outcomes .

[G 5] This step is a new iteration of the monitoring process, using as inputs the outcomes of the action plan or the new outcomes of the processes modified by the action plan.

[G 6] In this step it also might be needed to reflect on changing the existing design of the monitoring to adapt it to the implemented measures. Indeed, it is worth reflecting on the option for improving the existing design of the management system, including the analysis of whether the strategy, priorities and plan(s) for the monitoring activities need to be changed in order to carry out monitoring in a more efficient way.

[G 7] Experience from an earlier iteration of the monitoring process, is also one important part of continuous improvement.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

7. Evidence from the application of the monitoring process

7.1. The monitoring process shall be documented to prove it has been applied correctly. This documentation shall be made available primarily for internal assessment purposes. Upon request:

(a) railway undertakings and infrastructure managers shall make this documentation available to the national safety authority;

(b) entities in charge of maintenance shall make this documentation available to the certification body. If interfaces are managed through contracts, the entities in charge of maintenance shall make this documentation available to the respective railway undertakings and infrastructure managers.

7.2. The documentation produced under point 7.1 shall include in particular:

(a) a description of the organisation and staff appointed to carry out the monitoring process;

(b) the results of the different activities of the monitoring process listed in Article 3 (2) and in particular the decisions made;

(c) regarding instances of identified non-compliance that are considered unacceptable, a list of all necessary measures to be implemented to achieve the required outcome.

[G 1] As part of the management system, all the documentation related to the monitoring process needs to be treated in accordance with the internal procedures defined within the management system.

[G 2] The evidences from the application of the monitoring process need to be included in the annual safety report compiled by the railway undertakings, infrastructure managers and entities in charge of maintenance.

[G 3] The documentation produced during the application of the process needs also to be configured taking into account the following elements defined in the management system:

(a) document management system;
(b) management system documentation;
(c) criteria and formats for internal and external communication;
(d) involvement of staff and their representatives;
(e) configuration control of safety information.

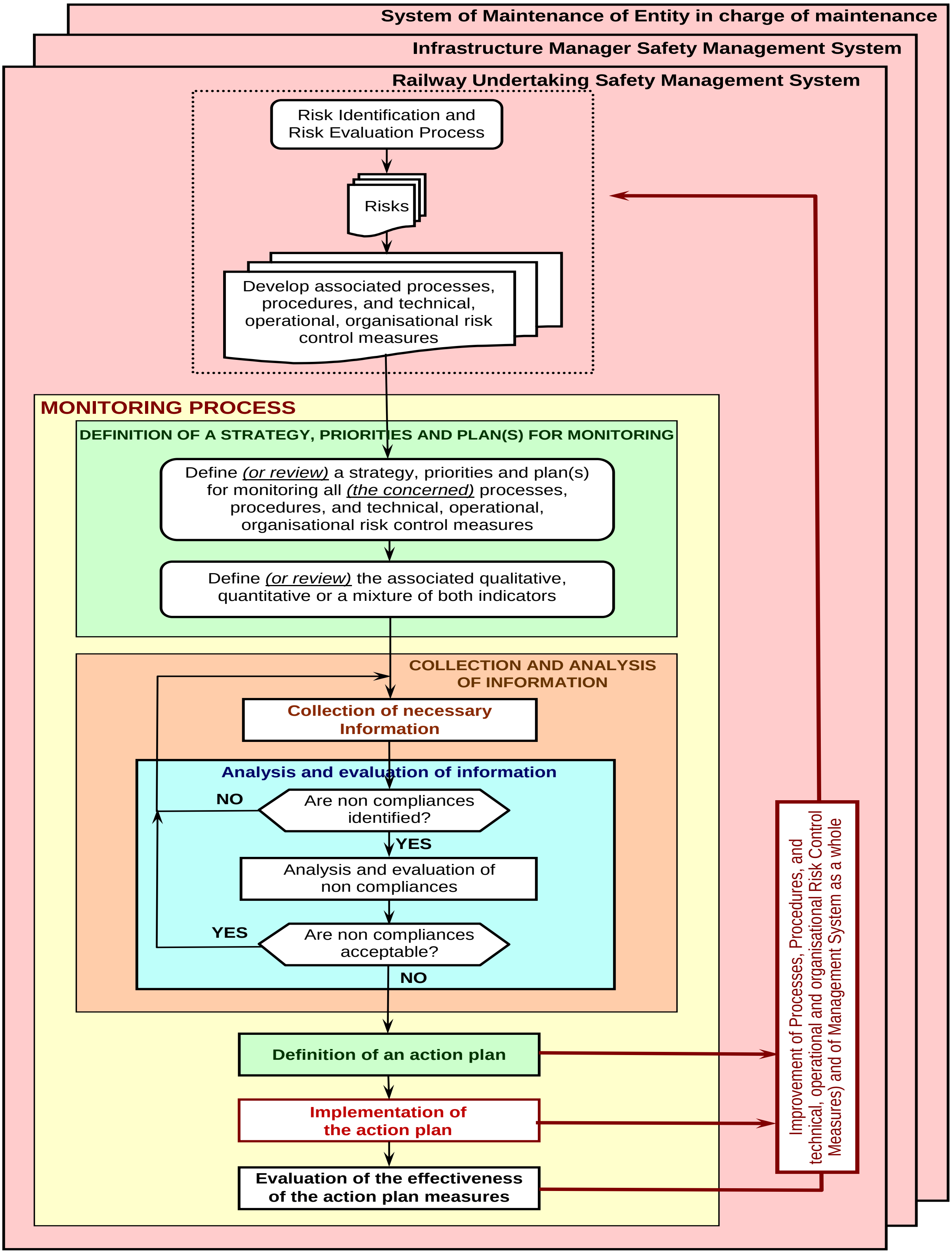
[G 4] A proper level of traceability needs to be established in setting up the format of the documents produced. The essential elements to be considered for the traceability requirements are at least:

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) formal approval of the monitoring procedures;
(b) budget and resources assigned for monitoring activities;
(c) responsibilities assigned and accepted;
(d) decisions made concerning the implementation of action plans;
(e) formal approval of the action plans;
(f) budget and resources assigned for the action plans.

The traceability is useful to analyse past actions when changes need to be done. The analysis can provide a better understanding of possible problems or it can be helpful when risk assessments need to be performed according to the CSM for risk assessment. Also, when the corrective/preventive measures contained in the action plan are not effective, keeping traceability of all changes and decisions enables analyses to be carried out in order to better understand the reasons for that and to identify a more appropriate action plan.

Appendix - Framework for the monitoring process



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

APPENDICES TO THE GUIDE WITH ILLUSTRATIVE EXAMPLES OF DIFFERENT STEPS OF THE MONITORING PROCESS

1. Example 1: Design of monitoring by a Railway Undertaking

1.1. Context of the example

Table 17: Design of monitoring by a Railway Undertaking.

Kind of railway actor	Railway undertaking
Articles and/or sections in the Annex of Regulation 1078/2012 that the example most closely relates to	The example is mainly connected to Article 1(2) and section 2 in the annex of Regulation 1078/2012
Description of the example, including among others: • its scope; • how it fits within the overall monitoring framework; • a brief summary of the content; • any limitations: *all process steps are not shown, all details of the process step are not presented; only examples are shown, etc.;* • who uses the example; • other relevant information	The example illustrates how a railway undertaking can identify the indicators to be used for monitoring the safety performance of its activities. It is pointed out that: • the definition of the indicators must be adapted to the specificities of every company and the particularities of its SMS. The company organisation, operation, processes, tasks, company management, etc. are different from company to company. All those company characteristics condition the indicators to be used for monitoring the safety performance of its safety management system; • the example is not exhaustive. The indicators cannot be copied and pasted. The example illustrates nevertheless how the indicators can be defined in an exhaustive and systematic way; • the methodology used in the example is not the only possible approach to define indicators. Other ways of identifying indicators are also possible.
How could it be used by other actors?	This method for defining indicators could be used by other companies. But it should be applied taking into account the specificities of the activities and of the SMS of every company.

1.2. Introduction

[G 1] This example illustrates the implementation of a monitoring process by a railway undertaking. The monitoring activities of the example are set up based on the outputs of the risk assessment and risk management performed at the setup of the company

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

safety management system. It is a proactive monitoring process that measures the safety performance of the operational processes of the company. It enables to detect non-compliances at an early stage and to take corrective and/or preventive measures before they escalate into accidents, incidents, near-misses or other dangerous occurrences.

[G 2] The complete monitoring process from the railway undertaking is not reported and described in this document. Only the definition of a strategy, priorities and plan(s) part of the monitoring process is illustrated to a given extent of details.

[G 3] This example does neither provide a complete list of indicators nor a complete list of defined rules, tools etc. which might be necessary for monitoring effectively the safety performance of the company.

1.3. Description of the company

1.3.1. Short description and type of activity

[G 1] Freight Rail is a newcomer railway operator with freight transportation as business core activity.

[G 2] Freight Rail is not operating in foreign countries.

1.3.2. Organisation of the company

[G 1] Freight Rail has 60 employees in total, including the management and the operational staff.

[G 2] The internal organisation of the company is shown in Figure 13 where the responsibilities are as follows:

(a) The **CEO** is accountable to the Administration Board of the company for the railway undertaking business in terms of "Health, Economic performance and Legal obligations";

(b) The **SMS Manager** is responsible for designing and supporting the implementation of the SMS within the company. He/she has also the responsibility for monitoring the overall safety performance. He/she is accountable to the CEO for reporting the safety performance and for identifying any possible continuous improvement;

(c) The **Rolling Stock Manager** is responsible for the maintenance procedures and planning the maintenance of the rolling stock;

(d) The **HR Manager** is responsible for complying with all legal procedures related to the employees, including the management of necessary health checks;

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(e) The **Production Director** is accountable to the CEO for the Operations in terms of "Health, Economic performance and Legal obligations". The occupational health is not part of the SMS.

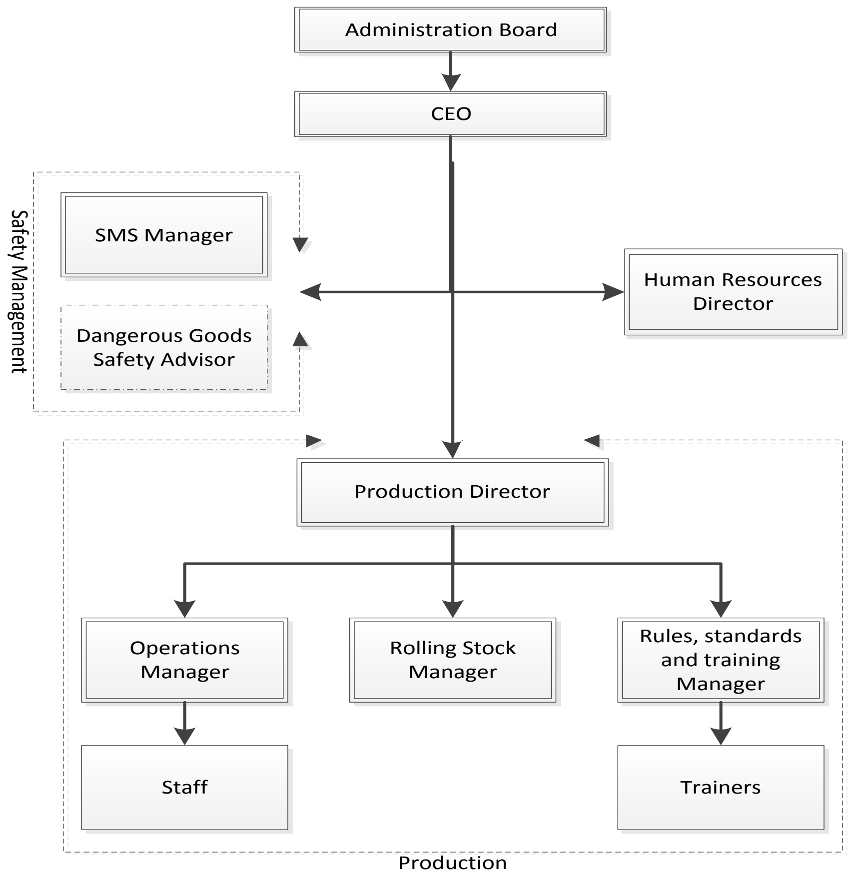


Figure 13: Organization chart of Freight Rail.

1.4. Processes defined within the company

[G 1] The processes within the SMS that are relevant for the example are:

(a) Operations;
(b) Monitoring;
(c) Staff Recruitment and Training;
(d) Document management and communication;
(e) Risk Management.

European Railway Agency • Rue Marc LEFRANCQ, 120 • BP 20392 • F-59307 Valenciennes Cedex • France • Tel. +33 (0)3 27 09 65 00 • Fax +33 (0)3 27 33 40 65 • http://www.era.europa.eu

1.5. Designing monitoring

1.5.1. Introduction

[G 1] The definition of the monitoring activities in this company started with the definition of a strategy. The strategy for monitoring includes:

(a) the decisions on how the SMS processes have to be monitored;
(b) the tools to be used for the monitoring activities;
(c) the tools necessary to arrive at decisions;
(d) the description of the level of involvement of the technical and operational expertise within the monitor activities.

1.5.2. Strategy for monitoring

[G 1] The strategy for monitoring is defined taking into account the safety policy approved by the CEO. A short part of the safety policy is reported below:

"…to preserve the business it's crucial to avoid accidents, especially during the start up of the company…"

[G 2] As a consequence of the company safety policy, the company goal is to build a "proactive monitoring process" that will raise warnings as early as possible before accidents, incidents, near-misses or other dangerous occurrences happen. The strategy adopted to achieve this goal can be summarised in the following points:

(a) prioritisation of the monitoring activities;
(b) set up of the tools for collecting monitoring information and data (e.g. audits, inspections, hierarchical checks, etc.);
(c) set up of indicators;
(d) definition of data streaming within the company;
(e) definition of the tools/rules for the review of the safety performances by the high level management;
(f) definition of the tools/rules for the definition and implementation of corrective and/or preventive measures to be included in the action plan.

1.5.3. Prioritisation of the monitoring activities

[G 1] All the processes of the SMS need to be monitored in order to check whether they are actually implemented and whether they are effective[9]. At least two different approaches can be used to prioritise the monitoring of the safety performance of the SMS processes. These two approaches provide different level of accuracy and a different level of details:

(a) setup of monitoring based on the outcomes of a risk assessment;

(b) setup of monitoring based on technical expertise of the company.

[G 2] For defining the monitoring activities, Freight Rail mixed those two approaches for monitoring the safety performance in function of the SMS processes:

(a) for the core processes (operations), the company decided to use the results of a risk assessment;

(b) for the other processes, the company decided to use the approach based on its technical expertise;

An example of definition of indicators based on the expert judgment is indicators for monitoring the Risk Control Measures (RCM) included in the training process.

[G 3] These two approaches for setting up the priorities for the monitoring activities are detailed in the next paragraphs of this document.

1.5.4. Setting up of tools for collecting monitoring information and data

1.5.4.1. Introduction

[G 1] Freight Rail uses different tools for collecting monitoring information and data. They are in line with Directive 2004/49/EC. In this example, Freight Rail used the following tools:

(a) internal audits, as required by criterion S in Annex II of Regulation 1158/2010 and basic element 2(j) in Annex III of Directive 2004/49/EC;

(b) investigations, as required by criterion Q of Regulation 1158/2010 and basic element 2(h) in Annex III of Directive 2004/49/EC;

---

(9) *Checking the effectiveness of an SMS process means verifying on the field, i.e. during the operation of the SMS, whether the considered process is successful in controlling the associated risk(s) to the level which was expected to be met when the safety management system was set up.*

(c) hierarchical checks, as required by criterion G in Annex II of Regulation 1158/2010;

(d) feedback from the staff, as required by criterion H in Annex II of Regulation 1158/2010.

[G 2] The "monitoring tools" are classified in two groups:

(a) **Group #1:** it includes internal audits, investigations and hierarchical checks.

The use of these tools is planned with managers and employees. They are the basic elements for collecting data in a systematic way. Compliance with the planned activities can also be easily monitored or checked whether they took place;

(b) **Group #2:** it includes feedback from the staff.

The use of this tool can be foreseen, but its actual use cannot be planned because the inputs are dependent on reporting from the staff. Consequently, its implementation cannot be monitored. But it is important to implement it in order to set up a direct feedback from the field.

1.5.4.2. Internal Audits

[G 1] An audit plan is annually defined by the SMS Manager. It is approved by the CEO.

[G 2] In the first year of existence of Freight Rail, the plan foresees auditing of the organisational structure of the company and of all SMS processes.

[G 3] Then, the plan foresees that for every further year of operation, the audit plan takes into account the results of the audits performed during the previous years. If a specific process/activity performs badly last year, from the safety point of view, more attention will be given to this process/activity with a more frequent audit activity.

[G 4] A dedicated procedure for planning and executing audits is defined in the company SMS.

1.5.4.3. Investigations

[G 1] The investigations are by default a reactive tool that cannot be planned[(10)].They are to be undertaken on occurrence of unexpected accidents, incidents, near-misses or other dangerous occurrences.

[G 2] Their purpose is to understand the actual causes of the accidents, incidents, near-misses or other dangerous occurrences in order to improve the SMS processes and to avoid the occurrence of similar events in future.

[G 3] Investigations are also considered as part of the monitoring process. A dedicated procedure for investigations is defined in the SMS of the company.

[G 4] Investigation should explicitly identify deficiencies in the safety management system, if applicable.

1.5.4.4. Hierarchical checks

[G 1] The hierarchical checks are a direct consequence of the manager's responsibility. The purpose is to check, at every level of the company organisational structure, that the SMS processes are actually implemented by the staff.

[G 2] Hierarchical checks are also a planned activity. The managers are requested to control if the organisational structure they are responsible for works in compliance with the company rules and standards.

[G 3] The hierarchical checks are structured in two levels:

(a) the manager checks whether:

   (1) the SMS procedures and activities are correctly implemented and executed, and;
   (2) the SMS procedures and activities are effective;

(b) the CEO checks that the managers' checks are performed at the different levels through the company organisation.

---

(10) *If the monitoring process is well designed and proactive enough, before an accident or an incident actually occurs, the application of the monitoring arrangements will raise early warnings and enable preventive actions to be taken before the accident or incident occurs.*

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.5.4.5. Feedback from the staff

[G 1] As mentioned earlier in this example, this tool cannot be considered as a systematic way for gathering monitoring information. It is nevertheless important to have in the SMS a dedicated procedure for describing the way staff can report non-compliances observed on the field. Freight Rail opted for an anonymous reporting of events by operational staff. The management objective is to involve, with this tool, the operational staff in the overall management of safety and to improve their self-consciousness of the hazards they are facing and managing.

[G 2] The actual involvement of the staff and the effectiveness of this tool depend therefore on the trust given from the staff to the company for using their feedback to actually improve the company safety management system and not for taking actions against the involved staff. A lack of trust in the use of the data automatically results in low rate of reporting non-compliances.

[G 3] The staff also pays a different attention in function of whether they report non-compliances or violations of company rules and standards. Most of the time, the subjective perception of the hazard may push the operational staff to report only events that they consider dangerous.

[G 4] Due to this subjectivity, all the monitoring information reported by the staff is analysed by the managers at the different levels of the organisational structure, helped by the company SMS manager.

1.5.5. Setting up indicators

1.5.5.1. Introduction

[G 1] The different types of indicators for monitoring the operational functions come from the following different sources:

(a) European legislation: Common Safety Indicators;

(b) National legislation: indicators defined by law in the Member State;

(c) Company rules: internal indicators defined taking into account the company needs and targets.

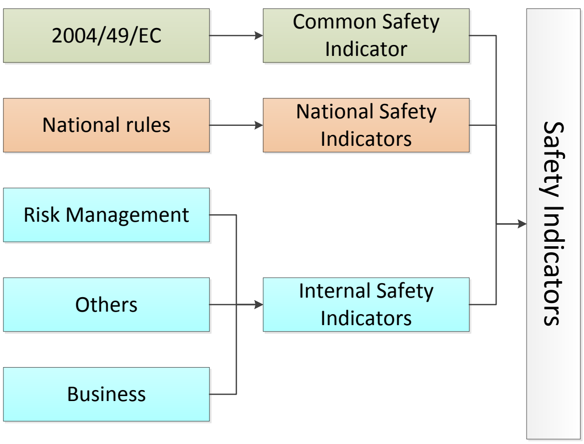


Figure 14: Sources of indicators for the monitoring.

1.5.5.2. Indicators available within the European legislation

[G 1] Indicators that must be used are required in Directive 2004/49/EC, particularly important are the amendments introduced by the Directive 2009/149/EC. An example is the "number of train derailments".

1.5.5.3. Indicators provided by the national legislation

[G 1] In the Member State where this example comes from, a National Safety Law defines a national "set of indicators" also to be monitored. Compliance with that national law is therefore mandatory. Those indicators are also to be reported within the monitoring process.

1.5.5.4. Internal indicators

1.5.5.4.1. Setup of monitoring based on the outcomes of a risk assessment

[G 1] Freight Rail applies the risk assessment and risk management process defined in their SMS[11]:

(a) to identify all the hazards, and related risks, that are linked to their operations, and;

(b) to define organisational, operational and the use of technical risk control measures.

[G 2] A secondary use of the result of risk assessment is the identification of the associated indicators specific to the company operations that are to be monitored in order to verify the compliance with the safety performance requirements. The company is now aware of the risks and free to decide what needs to be monitored in details and how.

[G 3] The company management is involved in the risk assessment, in particular during the hazard identification phase. Then, <u>for each identified hazard</u> the following is done:

(a) a Fault Tree Analysis (FTA) is performed to find out the potential causes for the identified hazards.

---

(11) *Freight Rail uses Regulation 402/2013 {Ref. 14} for the risk assessment of significant technical, operational and/or organisational changes. For all other types of changes or risk assessments, Freight Rail uses the ISO 31000 standard. This latter one matches all the steps of the risk assessment process in Annex of Regulation 402/2013 except that it does not require the use of an assessment body.*

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) the associated risk is evaluated in compliance with the applicable National Safety Rules: "acceptable risk", "tolerable risk" or "not acceptable risk".

(c) every hazard is given a Risk Priority Number (RPN) in order to enable the company to prioritise the risk management and to focus the risk assessment efforts upon the most important risks to be controlled.

The Risk Priority Numbers provide information about the severity consequence of the associated risk. It is defined between 0 and 1. A higher RPN means a higher risk associated to the hazard (higher likelihood or more severe consequence or both).

In this example, Freight Rail uses also the RPN as support to setup priorities for the monitoring activities within the company.

(d) the risk control measure that moves the risk from the "not acceptable" into the "tolerable or acceptable" area;

(e) the setup of indicator(s) that enables to monitor the effectiveness of the selected risk control measures

(f) the results from the risk assessment are registered in a Hazard Record/Log for further risk management, including:

(1) the identified hazards,
(2) the associated risks,
(3) the Risk Priority Numbers (RPN),
(4) the resulting safety requirements (i.e. risk control measures) to be implemented,
(5) the person responsible for the correct application of the safety requirements,
(6) the indicator(s) enabling to measure the effectiveness of the selected risk control measure,
(7) the person responsible for monitoring the indicator(s).

[G 4] Many indicators have been identified in the scope of this risk assessment. However, for the purpose of this example, in order to increase the readability of the document, the list is intentionally shortened. Table 18 below gives an extract of the identified indicators for the monitoring.

[G 5] For the purpose of this example, all the hazards linked to shunting operations (i.e. lines 6, 7 and 33 in Table 18) of the risk assessment, which have also the highest RPN, are considered below: see Table 19.

[G 6] To analyse further the potential causes of those hazards using a Fault Tree Analysis (FTA), all the hazards related to shunting operations are grouped in the unwanted top event "Hazards in Shunting Operations". The FTA is shown in Figure 15.

Table 18: Example of indicators for safety performance monitoring,

ID	Indicator
1	Locomotive running without permission
…	…………
6	Shunting operation not authorised
7	Wrong shunting operation
8	Wrong consistency of the train
9	Rear-End Train Lights malfunction
10	Wrong brake system settings
…	…
33	Irregular shunting operation
34	Unwanted train movement

Table 19: Selected hazards grouped for the FTA.

ID	Hazard	Classification	RPN
6	Shunting operation not authorised	Tolerable	0,1990
7	Wrong shunting operation	Tolerable	0,2141
33	Irregular shunting operation	Tolerable	0,1371

[G 7] The hazards registered in the Hazard Log are precursors of this top event. The Fault Tree Analysis built during the risk assessment models the main causes that lead to these precursors.

[G 8] Based on their expert judgement, the Operation Manager, supported by the SMS Manager, reviews the results from the risk assessment and decides which of the identified hazards need to be monitored.

[G 9] The Fault Tree Analysis (FTA) shows clearly two different types of events that contribute to the unwanted top event:

(a) intermediate events (see Table 20);
(b) basic events.

[G 10] For the considered top event ("hazards in shunting operations"), the "basic events" show the links with the other processes of the SMS (e.g. training). The "intermediate events" (see Table 20) provide details about the causes of the top event. Considering the intermediate events also as unwanted outcomes, the Operation Manager, supported by the SMS Manager, sets up specific indicators to monitor:

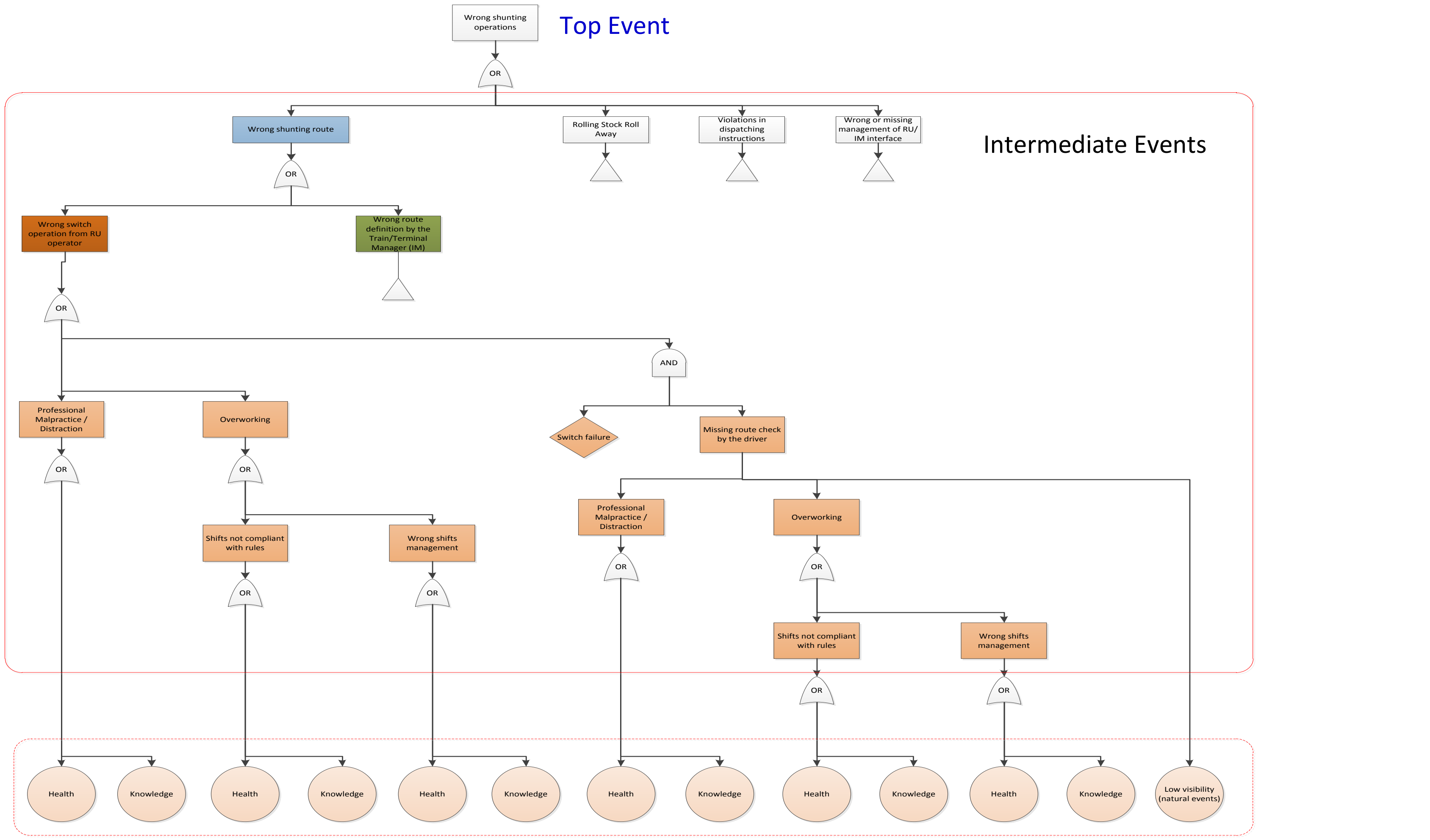


Figure 15: FTA for the "hazards in shunting operations".

Table 20: Intermediate events within FTA of "hazards in shunting operations".

ID	Top Event	Intermediate Events
SH_1	Hazards in Shunting Operations	Wrong switch operation from RU operator
SH_2	Hazards in Shunting Operations	Professional Malpractice/Distraction
SH_3	Hazards in Shunting Operations	Overworking
SH_4	Hazards in Shunting Operations	Shifts not compliant with rules
SH_5	Hazards in Shunting Operations	Wrong shifts management
SH_6	Hazards in Shunting Operations	Missing route check by the driver
SH_7	Hazards in Shunting Operations	Competence Maintaining System of the IM

[G 11] **Therefore, setting up indicators for the causes of the considered top event, *itself being a precursor of a higher level unwanted event*, enables Freight Rail to monitor the occurrence of unwanted events in a proactive way and to take on time corrective and/or preventive actions so that the unwanted event does not occur.**

1.5.5.4.2. Setup of monitoring based on the company technical expertise

[G 1] Section § 1.5.5.4.1 describes how Freight Rail identifies the basic events or basic causes that lead to the considered unwanted top event *("hazards in shunting operations")*. For the purpose of this example, those basic events are used to identify in which processes of the SMS or parts of a process of the SMS a barrier is to be defined and monitored in order to reduce the occurrence or the severity of the top event.

[G 2] Taking into account the risk priority numbers (RPNs) from the risk assessment, Freight Rail prioritises the risk control measures and monitoring activities to the areas of operation that give rise to the greatest risks.

[G 3] Based on the risk priority numbers (RPNs) and the Fault Tree Analysis (FTA) in Figure 15, Freight Rail concludes that the following basic events are to be monitored.

Table 21: Basic Events

ID	Top Event	Basic Events
SH	Hazards in Shunting Operations	Health issues
SH	Hazards in Shunting Operations	Knowledge issues
SH	Hazards in Shunting Operations	Low visibility
SH	Hazards in Shunting Operations	Interface with IM's SMS not working or missing
SH	Hazards in Shunting Operations	Switch Failure

[G 4] The identified basic events point out the importance of "staff competence, a continuous compliance with the applicable rules and a good management of the interfaces with other actors". The identification of those basic events enables the Operation Manager and SMS Manager to determine which processes of the SMS need appropriate risk control measures to be implemented, and therefore also to be monitored. The definition of the indicators for monitoring those processes results from the analysis of those SMS processes.

[G 5] The formal risk assessment was performed only for some of the processes of the company SMS.

[G 6] For the other processes of the SMS, the definition of the necessary risk control measures, and of the associated indicators, was done differently. The Operation and SMS Managers organised brainstorming meetings with multidisciplinary experts of the company. The results were formally documented in a report of the meeting. During these brainstorming meetings, the related processes were analysed and complemented with requirements (i.e. risk control measures) to make the risks acceptable. Relevant indicators for monitoring were also set up for checking the correct application and effectiveness of SMS processes and risk control measures.

[G 7] The results from the risk assessment and the results from the brainstorming meetings are registered in a **Hazard Record/Log** for further risk management, including:

(a) the identified hazards,
(b) the associated risks,
(c) the resulting safety requirements (i.e. risk control measures) to be implemented,
(d) the person responsible for the application of the safety requirements,
(e) the indicator(s) enabling to measure the effectiveness of the selected risk control measure,
(f) the person responsible for monitoring the indicator(s).

[G 8] The results from the Fault Tree Analysis (FTA) show that most of the basic causes that lead to "wrong shunting operations" are connected in practice to the **health, knowledge and motivation of the staff**. Consequently, the following processes of the SMS were also analysed and improved with additional requirements (i.e. risk control measures):

(a) the "Recruitment Process" as it needs to check that the recruited workers fulfil the competence requirements necessary for the company, and;

(b) the "Training Process" as it needs to ensure the competence is continuously available, and updated when necessary, in the company.

[G 9] Some parts of these two processes are prescribed by the national law of the Member State. The details of the other parts that are not prescribed *(e.g. recruitment requirements, actual training programs and procedures for exams)* are improved, based on the results of the risk assessment and brainstorming meetings, to make the overall risk acceptable.

[G 10] The specified frequencies for the "health checks", "skill checks" and "training checks" are:

(a) "risk control measures" that need to be implemented for keeping the associated risks under control, and;

(b) indicators for monitoring that enable to verify that the SMS processes are correctly implemented and effective in achieving the specified safety performance.

[G 11] Figure 16 below represents all the activities that are contained in the training process of the SMS. The red boxes are the "risk control measures" to be put in place in the training process to avoid the occurrence of the basic causes that are identified in the Fault Tree Analysis (FTA) in Figure 15.

[G 12] Here is an example of the analysis by a group of experts of the training process. The different steps of that process are represented in Figure 16. Only a short part of the complete analysis is reported here. Each step or activity of the training process is analysed and specific indicators are set up for monitoring the correctness of the application of the risk control measures and their effectiveness in achieving the expected safety performance:

(a) **Recruitment – Selection of workers**:

This is a formal step where the education, the professional experience and the knowledge of all the candidates are assessed. The workers recruited for the operational activities must comply with all the competence requirements that are setup either by national legislation rules or by the Operation Manager;

<u>**Defined indicators:**</u> number of selected workers that are not compliant with the competence requirements;

(b) **Qualification – Exam 1**:

This is a theoretical check of the staff competence and staff knowledge at the end of the training course. Its purpose is to check whether the operational worker knows, understands and is able to comply with all the operational requirements. Monitoring the exams enables to monitor:

(1) the check of the necessary worker's aptitude (e.g. health certificate, qualification certificate, etc.) and assessment of that documentation;
(2) the correct assessment of the worker competence, and;
(3) the correct organisation of the training activity itself in terms of training length, training implementation and training effectiveness.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Defined indicators: number of missing or wrong checks of the attendance list, wrong training session length, number of missed checks and number of missing documentation regarding the workers' health checks and workers' qualifications.

(c) **Qualification – Exam 2:**

The purpose of this step is to verify on the ground the effectiveness of the practical training. This step uses the same indicators as those defined in the previous step.

Defined indicators: number of missing or wrong checks of the attendance list, wrong training session length, number of missed checks and number of missing documentation regarding the workers' health checks and workers' qualifications.

(d) **Maintaining the worker competence – Health checks:**

Workers' health issues are among the most recurrent causes of failures during the operational activities. The barrier defined to avoid its occurrence is a periodic health check. The scheduling of health checks is defined using software that generates warnings in case of wrong management of deadlines. The effectiveness of this barrier can be evaluated in terms of number of missed checks and in terms of health issues. It's important to underline that all the operators are subject to the same kind of health checks.

Defined indicators: number of missing health checks or number of wrong health checks, number of discovered health issues, number of examined operational workers.

[G 13] The setup of indicators for monitoring of the training process is the result of brainstorming meetings with the managers of the operational activities, staff, etc. The results of these brainstorming sessions are documented in compliance with the procedures that are defined in the SMS of the company.

Table 22: Indicators derived from risk control measures of the training process.

ID	Indicator
SH8	Number of selected people not compliant with requirements
SH9	Number of missing or wrong check of the attendance list
SH10	Wrong training session length
SH11	Number of missed check and documentation regarding health checks and requirements
SH12	Number of missing or wrong health check
SH13	Number of health issues
SH14	Number of operators wrongly inserted in the shift pattern without a complete check
SH15	Number of missed updates

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

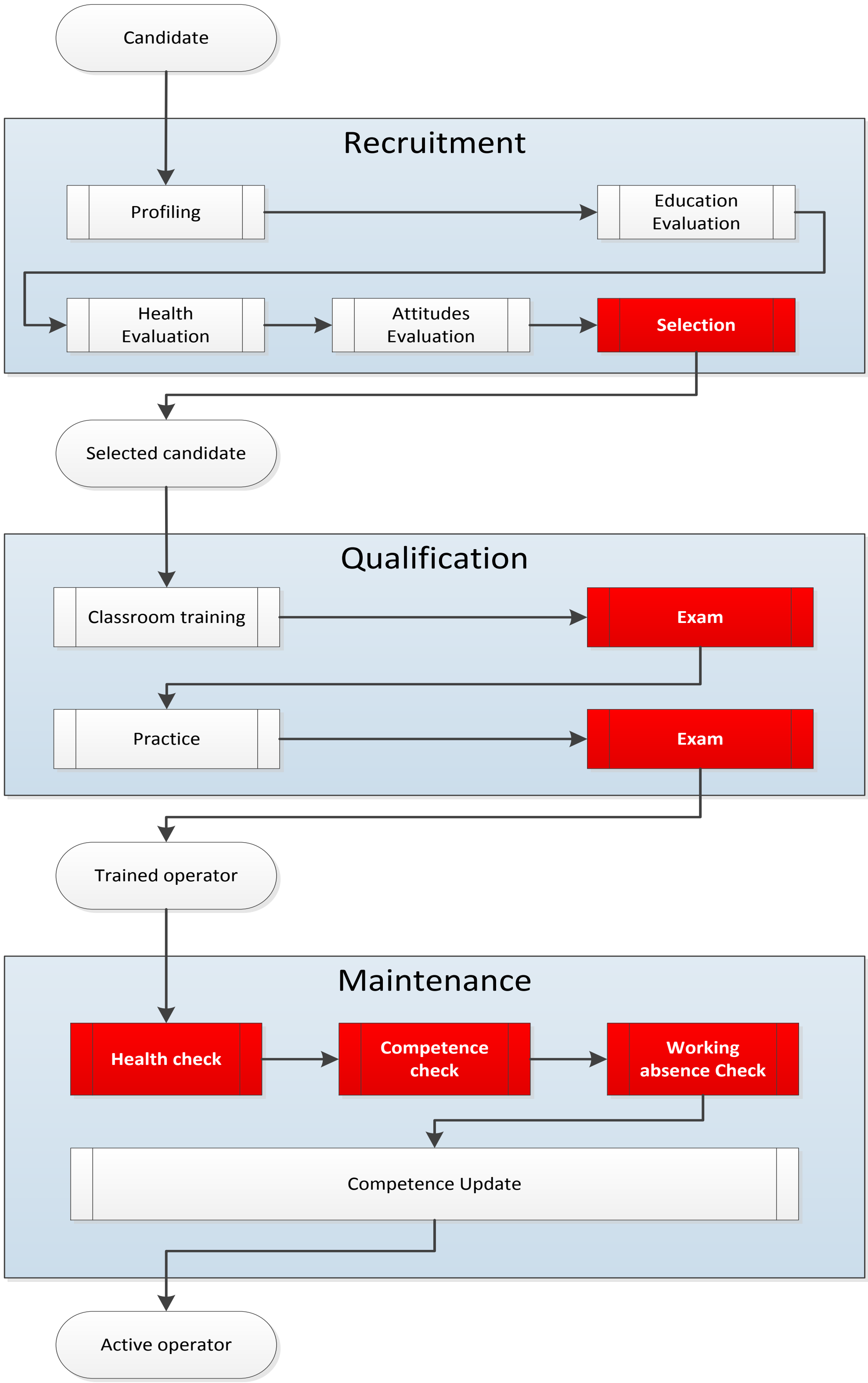


Figure 16: Training process.

1.5.5.5. Indicators related to the company specificities

[G 1] To follow the tendency of the safety performance in relation to the increase or decrease of business within the company, relative values are also used for indicators. Those indicators take into account the characteristics of the company in terms of number of employees, number of train*km, etc.

[G 2] Considering the indicators set up in the previous paragraphs, the indicators specified by National Legislation and those requested by the European Legislation, the following indicators are also defined:

Table 23: Indicators related to the company specificities.

ID	Indicator
R1	Number of Employees
R2	Number of Operational Staff
R3	Number of Health Check performed
R4	Number of “Long term” absences
R5	Number of Training activities
R6	Number of Exams
R7	Number of Train*Km
R8	Number of hours of shunting
R9	Number of Gross Tonne-kilometre moved
R10	Number of assigned shifts

1.5.5.6. Links between the indicators and associated risk control measures

[G 1] All the indicators setup in the previous paragraphs need to be clearly linked to the risk control measures they are referred to and whose effectiveness they enable to monitor. Table 24 below gives the correspondences.

Table 24: Links between the indicators and associated risk control measures

ID	Indicator	Definition
Internal Indicators from the Hazard Log relevant for the current example		
1	Locomotive running without permit	Locomotive used on a route on which running is not authorised. The indicator must be fed even in case the issue is detected during pre-departures checks.
….	…	…
6	Shunting operation not authorised	Shunting operations done without specific order. The indicator must be fed only if the operation has been done.
7	Wrong shunting operation	Mistakes in shunting operations. The indicator must feed only if the operation has been done.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table 24: Links between the indicators and associated risk control measures

ID	Indicator	Definition
8	Wrong consistency of the train	The indicator must be fed if the event occurs. The indicator must be fed even in case the issue is detected during pre-departures checks.
…	…	…
32	(Not protected) Level crossing accidents	The indicator must be fed if the event occurs.
33	Irregular shunting operation	The indicator must be fed if the event occurs.
34	Unwanted train movement	The indicator must be fed if the event occurs.
Internal Indicators from the FTA relevant for the current example		
ID	**Indicator**	**Definition**
SH1	Wrong switch operation from RU operator	The indicator must be fed if the event occurs and the shunting operation has been done.
SH2	Professional Malpractice/Distraction	The indicator must be fed if the event occurs.
SH3	Overworking	The indicator must be fed if the event occurs.
SH4	Shifts not compliant with rules	The indicator must be fed if the event occurs.
SH5	Wrong shifts management	The indicator must be fed if the event occurs.
SH6	Missing route check by the driver	The indicator must be fed if the event occurs.
SH7	Competence Maintaining System of the IM	The indicator must be fed if the event occurs.
SH8	Selected people not compliant with requirements	The indicator must be fed if the event occurs.
SH9	Missing or wrong check of the attendance list	The indicator must be fed if the event occurs.
SH10	Wrong training session length	The indicator must be fed if the event occurs.
SH11	Missed check and documentation regarding health checks and requirements	The indicator must be fed if the event occurs.
SH12	Missing or wrong health check	The indicator must be fed if the event occurs.
SH13	Health issues	The indicator must be fed if the event occurs.
SH14	Number of operators	This is not and indicator in a traditional way. It's necessary to analyse data.
SH15	Number of absences longer than 3 months	This is not and indicator in a traditional way. It's necessary to analyse data.
SH16	Number of operators wrongly inserted in the shift pattern without a complete check	The indicator must be fed if the event occurs.
SH17	Number of missed updates	The indicator must be fed if the event occurs.
Indicators from National Legislation relevant for the current example		
ID	**Indicator**	**Definition**
…	…	…
Indicators from Directive 2004/49/EC amended by 2009/149/EC		
ID	**Indicator**	**Definition**

Table 24: Links between the indicators and associated risk control measures

ID	Indicator	Definition
49	Broken Rails	Any rail which is separated in two or more pieces, or any rail from which a piece of metal becomes detached, causing a gap of more than 50 mm in length and more than 10 mm in depth on the running surface.
…	….	….
69	Injured – Other people.	-
Indicators related to the company specificities (relative values)		
ID	**Indicator**	**Definition**
R1	Number of Employees	Number of people employed by the company.
R2	Number of Operational Staff	Number of people engaged in safety related activities on the field.
R3	Number of Health Check performed	Number of health checks performed on Operational Staff.
R4	Number of "Long term" absences	Number of absences longer than 180 days.
R5	Number of Training activities	Number of training activities related to the qualification of Operational Staff.
R6	Number of Exams	Number of exams given for qualification of Operational Staff.
R7	Number of Train*km	Means the unit of measure representing the movement of a train over one kilometre. The distance used is the distance actually run, if available, otherwise the standard network distance between the origin and destination shall be used.
R8	Number of hours of shunting	Number of hours of shunting activities.
R9	Number of Gross Tonne-kilometre moved	Unit of measure representing the movement over a distance of one kilometre of one tonne of hauled vehicles and contents. The weight of railcars is included, the weight of the locomotive is excluded, shunting is not included.
R10	Number of assigned shifts	Total number of shifts assigned.

1.6. Data analysis

[G 1] Once the monitoring information and data is collected, it needs to be analysed. The managers at different levels of the company, supported by the SMS Manager, are responsible for this analysis. Each manager evaluates the achievement of the specified safety level by its team within the organisational structure of the company.

[G 2] The purpose of the analysis phase is to:

(a) evaluate the correct application of the processes and operational activities described in the SMS of the company;

(b) evaluate the effectiveness of those processes and operational activities;

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) evaluate the achieved safety performances of the company organisational structures;

(d) measure the trends of the indicators, using relative values (refer to section § 1.5.5.5);

(e) check whether the value of the indicators exceeds the thresholds, when such thresholds are setup during the identification of the indicators.

[G 3] The output of the data analysis phase is a report with the following information:

(a) the numeric value of the indicator;

(b) the numeric relative value assumed by the indicator;

(c) the trend of the indicators evaluated in 6 months, 1 year, 2 years, 5 years;

(d) an analysis on the general trend of the safety level of the organisational structure of the company.

[G 4] Table 25 below gives an example of the data analysis for two indicators.

Table 25: Raw Indicators related to the company specificities.

ID	Indicator
SH12	Number of missing or wrong health check
SH13	Number of health issues

[G 5] The following data need to be collected in order to calculate the relative values:

Table 26: Raw Indicators related to the company specificities.

ID	Indicator
R3	Number of Health Check performed
R2	Number of Operational Staff

[G 6] **Evaluation of the effectiveness of the "health check" processes and procedures:**

(a) The analysis can be simplified by verifying the following:

(1) *Is the health check procedure applied?*

(2) *How many health issues for the operational staff were discovered by the health check during this year?*

(3) *How many health issues for the operational staff were discovered by the health checks during this year considering the total number of employees in the company?*

(b) In order to evaluate whether the procedure of "management of the health checks" is correctly implemented, the company uses the specific indicator SH12 which comes from a Fault Tree Analysis (FTA).

The Human Resource (HR) Manager is responsible for the final evaluation of the correct application of the procedure of "management of health check".

(c) To check the number of health issues discovered for the operational staff, the HR Manager analyses the information collected through the "SH13-Number of health issues" indicator.

(d) To check the number of health issues discovered for the operational staff in relation to the total number of operational staff, the HR Manager considers also the information collected through the "SH13-Number of health issues" indicator but calculates the relative value using "Number of Operational Staff".

[G 7] All the data analysed by the different managers of the company is collected by the SMS Manager (who assisted them during the analyses). The SMS Manager then further analyses all this data in order to form a global view of the safety performance level of the company.

[G 8] The analysed data is the input for the Safety Review.

1.7. Safety Review and definition of Action Plans

[G 1] The Safety Review can be considered as a junction between the data analysis and action plan. It is a decisional step where the company managers consider the outputs of the data analysis activity to make decisions for defining and implementing the necessary action plans.

[G 2] The Safety Review process is carried out through "safety meetings" of the Safety Group, composed of:

(a) the CEO;
(b) the Production Director;
(c) the SMS Manager;
(d) the different Managers of the organisational structure of the company;
(e) the relevant experts, when necessary.

[G 3] During these safety meetings, the company managers overview the safety performance of their organisational structure, pointing out at:

(a) the main discovered safety issues, and;
(b) a general trend of the safety performances of the structure, and;
(c) a proposal of an action plan in order to improve or to consolidate the safety performance of their structure.

[G 4] During the Safety Review, the company top managers are informed about the safety performances of the company and of each part of the organisational structure. They are expected to decide on the proposed action plans: they approve them, request amendments or reject the action plans proposed by the different managers. Decisions are also taken to allocate the necessary resources for the implementation of the action plans.

[G 5] In case the agreed action plans exceed the available budget(s), the company top managers prioritise their decision on the basis of the following elements:

(a) the risk priority numbers (RPN) of the risks that the action plan is intended to control;
(b) the experts' opinion;
(c) the significant changes associated to the considered process/activity;
(d) the non significant changes associated to the considered process/activity;
(e) the extent at which the action plan is already effective or not, or whether it is badly implemented (e.g. because of lack of funds, resources, etc.).

[G 6] The outputs of the Safety Review are minutes of meeting which contain:

(a) the list of participants;
(b) a brief description of what has been reported by the different managers of the organisational structure of the company. The report of each manager is included in an annex of the minutes of meeting;
(c) the list of the action plans proposed by the different managers of the organisational structure of the company;
(d) the list of the action plans approved by the top management, , the allocated resources, the planning for their implementation, the safety targets (i.e. the expected outcomes) and the responsibilities for their application;
(e) the review of the monitoring plans for including the decided corrective actions, checking their correct application and effectiveness.

1.8. Responsibilities

[G 1] The company **CEO** in accountable for the overall safety performance of the company. He is also responsible for the correct application of the monitoring strategy at all the levels of the organisational structure of the company except for the production.

[G 2] The **Production Director** is accountable for the correct application of the monitoring strategy in the production structure of the company. He is also responsible for assessing the correct application and the effectiveness of the hierarchical checks that are to be performed.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 3] The **Managers** at the different levels of the organisational structure of the company are responsible for the achievement of the safety performance by their part of the organisational structure. They are also responsible for the correct application of the hierarchical checks, for the data collection (through shared spread sheets, with selective write/read rights) and for analysing the feedback collected from the staff. Eventually the **Managers** are responsible for analysing the collected safety data in order to report the achieved safety performance of their structure to the immediate hierarchical superior.

[G 4] The **SMS Manager** of the company is responsible for supporting the different managers in the correct application of the monitoring system and in the analysis of the collected data. The **SMS Manager** is also responsible for supporting the high level managers in their checking of the safety performance and in defining the appropriate action plans.

[G 5] Concerning the collection of monitoring data and indicators, the responsibilities associated to each indicator are defined in the following table.

[G 6] Table 27 below provides the list of the indicators and the related responsibilities:

Table 27: List of indicators and related responsibilities for collecting data.

Internal Indicators from the Hazard Log		
ID	**Indicator**	**Responsible**
1	Locomotive running without permission	Operation Manager
…	…	…
6	Shunting operation not authorised	Operation Manager
7	Wrong shunting operation	Operation Manager
8	Wrong consistency of the train	Operation Manager
…	…	…
32	(Not protected) Level crossing accidents	Operation Manager
33	Irregular shunting operation	Operation Manager
34	Unwanted train movement	Operation Manager
Internal Indicators from FTAs		
ID	**Indicator**	**Responsible**
SH1	Wrong switch operation from RU operator	Operations Manager
SH2	Professional Malpractice/Distraction	Training Manager
SH3	Overworking	Operation Manager
SH4	Shifts not compliant with rules	Operation Manager
SH5	Wrong shifts management	Operation Manager
SH6	Missing route check by the driver	Operation Manager
SH7	Failure IM's Competence Maintaining System	Operation Manager
SH8	Number of selected people not compliant with requirements	Training Manager

Table 27: List of indicators and related responsibilities for collecting data.

SH9	Number of missing or wrong check of the attendance list	Training Manager
SH10	Wrong training session length	Training Manager
SH11	Number of missed check and documentation regarding health checks and requirements	Training Manager
SH12	Number of missing or wrong health check	Training Manager
SH13	Number of health issues	HR Responsible for Health checks
SH14	Number of operators	HR Responsible for Health checks
SH15	Number of absences longer than 3 months	HR Responsible for Health checks
SH16	Number of operators wrongly inserted in the shift pattern without a complete check (after 3 months absence)	Operation Manager
SH17	Number of missed updates	Training Manager
Internal Indicators from National Rules applicable to Operations		
ID	**Indicator**	**Responsible**
…	….	….
Internal Indicators from Directive 2004/49/EC amended by Directive 2009/149/EC		
ID	**Indicator**	**Responsible**
49	Number of broken Rails	Operation Manager
50	Number of track buckles	Operation Manager
…	….	….
Indicators defined in order to calculate relative values		
ID	**Indicator**	**Responsible**
R1	Number of Employees	HR manager
R2	Number of Operational Staff	HR manager
R3	Number of Health Check performed	HR manager
R4	Number of "Long term" absences	HR manager
R6	Number of Exams	Training Manager
R5	Number of Training activities	Training Manager
R7	Number of Train*Km	Operation Manager
R8	Number of hours of shunting	Operation Manager
R9	Number of Gross Tonne-kilometre moved	Operation Manager
R10	Number of assigned shifts	Operation Manager

1.9. Planning of the monitoring activities

1.9.1. Link with the Safety Plan

[G 1] The monitoring activities are planned in time. They are included in the company Safety Plan which is delivered every year to the national safety authority. The Safety

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Plan schedules, on an annual basis, all the activities defined by the company in order to improve or to consolidate the safety level of the company.

[G 2] In the considered country, the Safety Plan is also required by a national safety rule. According to that national safety rule, the Safety Plan needs to be updated every three months, based on the feedback from the monitoring of the safety performance. The intermediate progress needs also to be reported to the national safety authority in order to enable it to supervise the effective implementation of the Safety Plan.

1.9.2. Planning of collection of the monitoring information and data

1.9.2.1. Monitoring Plan

[G 1] Every year, the planning of collection of the monitoring information and data is defined in a document (i.e. the Monitoring Plan) that is annexed to the Safety Plan. In the considered country, a national safety rule requires the railway undertaking to deliver this Monitoring Plan to the national safety authority.

[G 2] Concerning the example described in this guide, the Monitoring Plan includes:

(a) the audit plan;
(b) the planning of the analysis of the results from investigations;
(c) the planning of hierarchical checks;
(d) the planning of the analysis of the feedback from the staff

1.9.2.2. Audit Plan

[G 1] As described in section § 1.5.4.2, an Audit Plan is annually set up by the SMS Manager. The Audit Plan is approved by the company CEO.

[G 2] As Freight Rail is a newcomer, during the first year all the levels of the organisational structure and all the SMS processes of the company are planned to be audited. The following years, the definition of the Audit Plan takes into account the results of the audits of the previous year.

[G 3] A specific procedure for planning and executing the audits is defined in the company SMS.

1.9.2.3. Planning of the analysis of the results from investigations

[G 1] As described in section § 1.5.4.3, the results of investigations of unexpected accidents, incidents, near-misses or other dangerous occurrences are transmitted to all the managers of the company in order to make them aware of potential faults, non-

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

compliances and possible improvements. The managers of the different levels of the organisational structure of the company are responsible for feeding the indicators related to the investigations.

1.9.2.4. Planning of hierarchical checks

[G 1] As described in section § 1.5.4.4, every manager is responsible for checking that all the tasks included in his/her organisational structure of the company are correctly implemented and executed. The schedule for the checks is defined by the relevant manager on basis of the frequency which is set up during the definition of the associated indicators. The hierarchical checks are supported by a checklist, used as a guideline, to allow the managers to judge on the suitability of the considered check during the execution of the planned hierarchical checks. The planning of the hierarchical checks is also included in the Safety Plan.

[G 2] In order to define the <u>frequency of the hierarchical checks</u>, and therefore to prioritise the monitoring activities, the following elements are considered:

(a) <u>**Kind of activity executed by the staff and detectability of potential risks:**</u>

The purpose of monitoring is to detect non-compliances of the correct application, correct execution and effectiveness of the SMS processes and procedures. However, an analysis of the causal sequence of failures that can lead to accidents, incidents, near-misses or other dangerous occurrences might include both:

(1) <u>"active or direct failures"</u>: these are unsafe events that can be directly linked to accidents, incidents, near-misses or other dangerous occurrences (e.g. an excessive over speed might result in a derailment). The detection of these failures is done by reporting the occurrence of the relevant accidents, incidents or errors.

and

(2) <u>"latent or dormant failures"</u>: these are non-direct failures that will result in accidents, incidents, near-misses or other dangerous occurrences <u>only when</u> they are <u>combined</u> to (an)other failure(s). These failures contribute thus to the unsafe outcome but may be dormant for a long time (days, weeks, or months) until, in combination with those other failures, they finally contribute to accidents, incidents, near-misses or other dangerous occurrences. The detection of these failures is not easy as there is no direct and visible consequence that can be monitored.

Both active/direct and latent/dormant failures need to be detected:

(3) events easily detectable are identified as events to be reported by the Operational Staff;

(4) events not easily detectable need to be checked more frequently in order to detect the non-compliances as early as possible and to take the necessary corrective or preventive actions.

As the company risk assessment files did not include systematically the information on the detectability of failures/hazards, the assessment of their detectability, and the definition of the associated monitoring frequency, is done during a meeting with the company managers and experts from the field.

(b) **risk priority numbers (RPN) of the associated hazards:**

The risk priority numbers (RPN) are used to classify the hazards and the related risk control measures (RCM). Intermediate events identified by fault tree analyses (FTAs) have no specific risk priority numbers.

(c) **expert judgment.**

The expert judgement on the failure/hazard detectability is then combined with the risk priority numbers (RPNs) to define the priorities **(i.e. frequencies)** for the monitoring activities.

[G 3] The definition of the frequencies of monitoring of the identified indicators by the relevant managers is provided in Table 28:

Table 28: List of indicators and associated frequency for checks.

Internal Indicators from the Hazard Log			
ID	**Indicator**	**RPN**	**Frequency (Manager Check)**
1	Locomotive running without permit	0,0585	Once a month
…	…	…	…
6	Shunting operation not authorized	0,1990	Once a week
7	Wrong shunting operation	0,2141	Once a week
8	Wrong consistency of the train	0,1329	Once a month
…	…	…	…
32	level crossing accidents (not protected)	0,2189	Once a month
33	Irregular shunting operation	0,1371	Twice a month
34	Unwanted train movement	0,1519	Once a month
Internal Indicators from FTAs			
ID	**Indicator**	**RPN**	**Frequency (Manager Check)**
SH1	Wrong switch operation from RU operator	N.A.	Once a month
SH2	Professional Malpractice/Distraction	N.A.	Once a month

Table 28: List of indicators and associated frequency for checks.

SH3	Overworking	N.A.	Once a month
SH4	Shifts not compliant with rules	N.A.	Once a month
SH5	Wrong shifts management	N.A.	Once a month
SH6	Missing route check by the driver	N.A.	On time
SH7	Competence Maintaining System of the IM	N.A.	Once a month
SH8	Selected people not compliant with requirements	N.A.	Once a month
SH9	Missing or wrong check of the attendance list	N.A.	Once a month
SH10	Wrong training session length	N.A.	Once a month
SH11	Missed check and documentation regarding health checks and requirements	N.A.	Once a month
SH12	Missing or wrong health check	N.A.	Once a month
SH13	Health issues	N.A.	Once a month
SH14	Number of operators	N.A.	Once a month
SH15	Number of absences longer than 3 months	N.A.	Once a month
SH16	Number of operators wrongly inserted in the shift pattern without a complete check	N.A.	Once a month
SH17	Number of missed updates	N.A.	Once a month
Internal Indicators from National Rules applicable to Operations			
ID	**Indicator**	**RPN**	**Frequency (Manager Check)**
…	…	…	…
Internal Indicators from Directive 2004/49/EC amended by 2009/149/EC			
ID	**Indicator**	**RPN**	**Frequency (Manager Check)**
49	Broken Rails	N.A.	N.A.
…	….	…	…
69	Injured – Other people.	N.A.	N.A.
Indicators defined in order to calculate relative values			
ID	**Indicator**	**RPN**	**Frequency (Manager Check)**
R1	Number of Employees	N.A.	Once a month*
R2	Number of Operational Staff	N.A.	Once a month*
R3	Number of Health Check performed	N.A.	Once a month*
R4	Number of “Long term” absences	N.A.	Once a month*
R5	Number of Training activities	N.A.	Once a month*
R6	Number of Exams	N.A.	Once a month*
R7	Number of Train*Km	N.A.	Once a month*
R8	Number of hours of shunting	N.A.	Once a month*
R9	Number of Gross Tonne-kilometre moved	N.A.	Once a month*
R10	Number of assigned shifts	N.A.	Once a month*
= In this case the check is performed in order to verify that the indicator is fed.			

1.9.2.5. Planning of the analysis of the feedback from the staff

[G 1] As described in section § 1.5.4.5, the feedback from the staff is collected anonymously through dedicated mailboxes. The reliability of this information is granted through a further analysis by the Operation Manager, supported by the SMS Manager and the Trainers.

[G 2] The analysis of the feedback from the staff is done at least once a month. The result of the analysis is traced and transmitted to all the managers of the company.

1.9.2.6. Summary of all planned monitoring activities

[G 1] Table 29 summarises the planned monitoring activities.

Table 29: Planned monitoring activities.

Tool	Planned	Frequency	Results
Monitoring Plan § 1.9.2.1	Yes	Every year	Traced, sent to the CEO, SMS Manager and all company managers
Audit § 1.9.2.2	Yes, Audit programme	One audit per month	Traced, sent to the CEO, SMS Manager and all company managers
Investigation § 1.9.2.3	Not planned	When occurs (as foreseen in SMS)	Traced, sent to the CEO, SMS Manager and all manager(s) involved in the accident/incident
Hierarchical checks § 1.9.2.4	Yes, checks programme	Up to the indicators Table 28	Traced, internal use, notice of the check must be sent to directors/CEO
Feedback from the staff - § 1.9.2.5	Yes, only the analysis	One analysis per month	Traced, transmitted to all the managers

1.9.3. Planning of data analysis

[G 1] In line with the strategy described in section § 1.6, the data analysis of the collected information is done on a monthly basis. Every manager of the organisational structure of the company analyses the data under its responsibility. The results are written down in a dedicated report.

[G 2] Every manager communicates the discovered non-compliances to its immediate superior.

[G 3] Every three months, the managers provide the results on the achieved safety performance in order to update the Safety Plan.

[G 4] The outputs of the data analysis are then taken into account for the Safety Review.

1.9.4. Planning Safety Review

[G 1] In line with the strategy described in section § 1.7, the Safety Review activity is managed by the SMS Manager who organises at least one meeting every three months.

[G 2] The final Safety Review meeting of the year becomes the basis for building the Safety Plan of the next year and for writing down the Annual Safety Report to be delivered to the national safety authority.

2. Example 2: Monitoring by an Infrastructure Manager

2.1. Context of the example

Table 30: Design of monitoring by an infrastructure manager.

Kind of railway actor	Infrastructure manager
Articles and/or sections in the Annex of Regulation 1078/2012 that the example most closely relates to	Using a core hazard for the company, the example illustrates all steps of the monitoring framework defined in the annex of Regulation 1078/2012.
Description of the example, including among others: • its scope; • how it fits within the overall monitoring framework; • a brief summary of the content; • any limitations: *all process steps are not shown, all details of the process step are not presented; only examples are shown, etc.;* • who uses the example; • other relevant information	One of the business objectives of an infrastructure manager is to offer train paths, and ultimately a safe and reliable timetable, to its customers, the railway undertakings (RUs). It is important that this activity, offering a safe and reliable timetable, is monitored so that the on-going business activity can be undertaken in a safe manner. The example does not show every activity that it monitored by the infrastructure manager. It concentrates on the monitoring of risks associated with the "track quality". It is used in one European country and may be relevant to others for interest. The example describes how the infrastructure manager identifies the indicators to be used for monitoring the effectiveness of the risk control measures in place.
How could it be used by other actors?	It can be used by other actors as a slice of monitoring to show how the infrastructure manager can monitor the effectiveness of the risk control measures he puts in place to manage safely the railway traffic.

2.2. Introduction

[G 1] This example illustrates the correct application of the monitoring process by an infrastructure manager on a small part of the infrastructure. The monitoring activities of the example are set up based on the company return from experience. It is a proactive monitoring process that checks that the safety characteristic of the infrastructure do not exceed the tolerances permitted by the applicable standards. The process enables to detect non-compliances at an early stage and to take corrective and/or preventive measures before they escalate into accidents, incidents, near-misses or other dangerous occurrences.

[G 2] The complete monitoring process from the infrastructure manager is reported and described in this document. But it is illustrated for only one core hazard of the

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

company. The example does not show all the hazards and associated risk control measures and indicators that are also monitored by the infrastructure manager.

[G 3] This example does neither provide a complete list of indicators nor a complete list of defined rules, tools etc. which might be necessary for monitoring effectively the safety performance of an infrastructure manager.

2.3. Designing the Monitoring

[G 1] In this example, the monitoring activities are not set up based on a risk assessment and risk management of the infrastructure manager activities but on the return of experience over many years. The infrastructure manager knows that in order to deliver a safe and reliable timetable, a safe and reliable track system is needed. So, for the purpose of this example, in order to illustrate the monitoring activities of the considered infrastructure manager, a few particular hazards are considered and followed through the company safety management system.

[G 2] There are many railway hazards associated with the track system. For the purpose of the example, the ones related to the quality of the "track geometry" are considered as example. Those hazards are specified in applicable standards.

[G 3] The hazards associated with the "track geometry", in the context of the business objective of a safe and reliable timetable, include "rough ride" and "derailment" sub-hazards. Both of these sub-hazards could lead to the consequence of injuring a person in the train. Furthermore, even if a derailment does not result in an injury it results in a delay of the train and in a loss of service on the concerned line. This means that the fundamental business objective of offering a safe and reliable timetable is not met.

[G 4] The estimated risk for not controlling these two sub-hazards ("rough ride" and "derailment") associated with the track geometry can then be considered significant and suitable for monitoring both in safety and business terms.

2.4. Strategy for Monitoring

[G 1] Track geometrical limits are set out in well-established standards. These limits are directly set to eliminate "rough riding" and "derailment". They have been established over many years by return of experience and as a result of investigations of accidents and incidents that happened in the past.

[G 2] The strategy for monitoring of the infrastructure manager is to compare the "actual geometry seen on the network" with the "geometry specified in standards". This can be done by visual inspection from track workers walking along the track, by ultrasonic inspection or by automated inspection with specially equipped trains. If "track geometry defects" are detected then various risk control measures are possible depending on the severity of the detected defects. These various risk control measures include the following possible solutions:

(a) stopping operations;
(b) imposing a temporary speed restriction;
(c) conducting repair or performing maintenance;
(d) full infrastructure renewal.

[G 3] It should be noted that stopping operations or imposing a temporary speed restriction both act against the business objective of a reliable railway, even though they reduce or eliminate the consequences, in terms of injury, of the hazards. For this reason they are primarily intended as interim or short term controls.

2.5. Setting Indicators and prioritisation

[G 1] Indicators are setup to monitor each aspect of the cycle of inspection and to lead to corrective actions and repairs. The indicators are selected on the basis of expert judgement and return of experience. The indicators are chosen so that all aspects of the management of the hazards can be monitored. These safety indicators might include:

(a) the number of inspections required versus the number of inspections performed;
(b) the number of trained and competent staff versus the required number;
(c) the number of defects, in terms of exceeding the limits specified in standards, identified and their severity.

[G 2] Further indicators related to the business objective (if providing train paths) might include:

(a) the time taken to rectify the discovered defects, which is an important indicator of the business performance of the railway, i.e. the ability to provide a safe and reliable timetable;
(b) repair work planned versus the available resources;
(c) the number of speed restrictions imposed.

[G 3] The number of indicators is chosen in proportion to the potential frequency of the hazard, to the magnitude of any resulting risk and in regard to the ease or difficulty of collecting reliable data against the indicator. Unreliable data or data that can vary from one period to the next one, due to external factors such as the weather, can cause an indicator to be misinterpreted and an incorrect action to be taken. In this case consideration should be given to normalising the data or using a moving annual average or other technique to provide meaningful information. If no reliable data can be collected then the indicator should not be used.

2.6. Data Analysis

[G 1] Trends in all of the indicators are then studied to determine if the track geometry itself, or the process to monitor and correct it, are being adequately maintained. This includes the check of whether indicators exceed any trigger points or whether an indicator moves towards a trigger point for a number of consecutive periods.

2.7. Safety Review and Definition of Action Plans

[G 1] Regular safety reviews of the results of the monitoring activities, of audits and of the investigation reports of accidents and incidents are done to confirm that:

(a) the current risk control measures are appropriate and effective;

or

(b) either the current risk measures need to be correctly implemented or further risk control measures are necessary. The company is learning and improving the management of risks.

[G 2] If the current risk control measures are not correctly implemented or are not effective, an action plan is taken to implement them correctly or additional risk control measures are identified. The event is taken into account in the learning process of the company in order to improve the safety management system and make the existing controls more effective.

[G 3] The effectiveness of the action plan is then evaluated through a new loop of the monitoring activities. This includes also compliance checks, management reviews, audits and safety reviews.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

3. Example 3: Monitoring by an Infrastructure Manager

3.1. Context of the example

Table 31: Design of monitoring by an infrastructure manager.

Kind of railway actor	Infrastructure manager
Articles and/or sections in the Annex of Regulation 1078/2012 that the example most closely relates to	The example illustrates all the articles and the Annex of Regulation 1078/2012 on the CSM for monitoring.
Description of the example, including among others: • its scope; • how it fits within the overall monitoring framework; • a brief summary of the content; • any limitations: *all process steps are not shown, all details of the process step are not presented; only examples are shown, etc.;* • who uses the example; • other relevant information	It is an example of a monitoring process applied by an infrastructure manager. Being responsible for the safety performance of its network, the infrastructure manager needs to have a permanent indication of the safety trends on its network and in particular of the safety performance trends of the traffic management. This example does not present all the processes and procedures of the safety management system of the company. The ones considered here are also not entirely described. All figures about accidents, incidents and trends are fictitious. They are to be read only as an aid for understanding the logics of the monitoring activities of the infrastructure manager.
How could it be used by other actors?	It is one possible approach for monitoring. It shows how an infrastructure manager can monitor the effectiveness of the risk control measures put in place to manage safely the railway traffic on the network.

3.2. Introduction

[G 1] The monitoring activities described in the example are managed by the Safety Management Department in the operational headquarter of the company, under the leadership of the Safety Manager, but with the support of the other departments of the company for their area of responsibility.

[G 2] The Safety Management Department is directly responsible for providing all the indicators and associated key figures to the top management as well as to the relevant company departments.

[G 3] The overall "key performance indicator" is measured and updated on a monthly basis by the Safety Management Department. It is made available to the whole company staff on the Intranet.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

3.3. Description of the company

[G 1] The infrastructure manager results from the separation of the historical state railways; it is the largest infrastructure manager in the considered country. It has an experience for almost 200 years of railway operation and management.

[G 2] For the purpose of the example, the following data is pertinent for the company:

Table 32: Data about the infrastructure manager in Example 3.

Parameter	Figure
Number of employees	17 000
Number of line kilometres	5 000
Number of Stations	1 000
Number of shunting locations	100
Number of signals	30 000
Number of switches	15 000
Number of bridges	6 000
Number of tunnels	200
Number of level crossings	4 000
Number of hot axel boxes detectors	500
Number of hydroelectric plants	10
Train kilometres/year	150 000 000 (150 millions)

[G 3] According to the national law, the Safety Manager is responsible for the achievement of the safety performance by the company. So the different branches of the company are required to provide the Safety Manager with the necessary information. There is also a regular exchange of information on the measured safety performance between the infrastructure manager and the railway undertakings that operate on its network.

3.4. Monitoring process

3.4.1. Introduction

[G 1] This example shows one way of implementing and applying a proactive monitoring process by an infrastructure manager. The process is based on:

(a) the return of experience over many years of existence of the company;
(b) the results of investigations of accidents and incidents that happened;
(c) risk analyses, audits and on-going monitoring of the key risks for the company;
(d) suggestions from staff for a continuous improvement of the process.

[G 2] The purpose of the process is to <u>monitor in a proactive way</u> all the hazards linked to the company activities and, in case of ineffectiveness of the associated risk control measures, to take corrective or preventive actions at the earliest possible stage

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

before the hazards lead to accidents, incidents, near-misses or other dangerous occurrences.

3.4.2. General overview of the monitoring process

[G 1] The identification of what should be monitored is based on Hazard Tree Analyses built from the risks linked to the infrastructure manager activities. A Hazard Tree starts from a top event (i.e. an accident, an incident, a near-miss or any other dangerous occurrence) and models down the different contributing causes that can lead to the considered accident, incident, near-miss or other dangerous occurrence. The analysis models both the accident precursors(12) and as far as possible the root causes. An example of a hazard tree is given in section § 3.5.7.

[G 2] The company identifies in this way:

(a) all the causes that can lead to the occurrence of hazards and risks related to infrastructure manager activities, and;

(b) all the indicators that are to be monitored.

The indicators to be monitored are included in the Safety Program of the company for the on-going year.

[G 3] The monitoring of the safety performance includes both:

(a) <u>proactive monitoring</u> which verifies the correct application and effectiveness of the processes and procedures contained in the safety management system of the infrastructure manager, and;

(b) <u>reactive monitoring</u> which measures the failures of those proactive measures to actually prevent accidents, incidents, near-misses or other dangerous occurrences.

The outputs of these two branches of the monitoring process are used to define an action plan that will correct the detected non compliances and improve the safety management system of the company.

[G 4] Figure 17 represents the monitoring process. It is a cyclical process which includes the following steps:

(a) the definition of the strategy and plan for monitoring;
(b) the collection of monitoring information and data as defined in the Safety Program;

---

(12) *"Accident precursors" are conditions, events and sequences of events that precede and lead up to accidents.*

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) the analysis of monitoring information and data;
(d) the definition of an action plan for correcting the identified non-compliances;
(e) the review of the monitoring strategy and requirements.

[G 5] The monitoring strategy is based on the specificities of the infrastructure manager activities. The results of the strategy definition, as well as of all the indicators to be monitored, are included in the Safety Program of the company. The strategy is reviewed and updated every year based on the experience and results of the monitoring activities from previous year.

[G 6] The monitoring activities are managed by the Safety Management Department in the operational headquarter of the company, under the leadership of the Safety Manager, and with the support of the other departments of the company:

(a) every department of the company is responsible for monitoring the safety performance of its part of the organisational structure and for taking all necessary corrective actions to achieve, and improve where needed, the safety performance in their area of responsibility;

(b) in close collaboration with the other departments of the company, the Safety Management Department is responsible for monitoring the overall safety performance and the evolution of the safety tendency in the company.

[G 7] The Safety Management Department is responsible for reporting different key performance indicators to the top management and to the other departments of the company:

(a) an overall set of "key performance indicators" that represent the overall safety performance, and therefore the achievements of the long-term developments by the company.
These “key performance indicators” are measured and updated on a monthly basis by the Safety Management Department. They are made available to the whole company staff on the Intranet.

(b) key performance indicators that represent the safety performance achieved by every department of the company.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

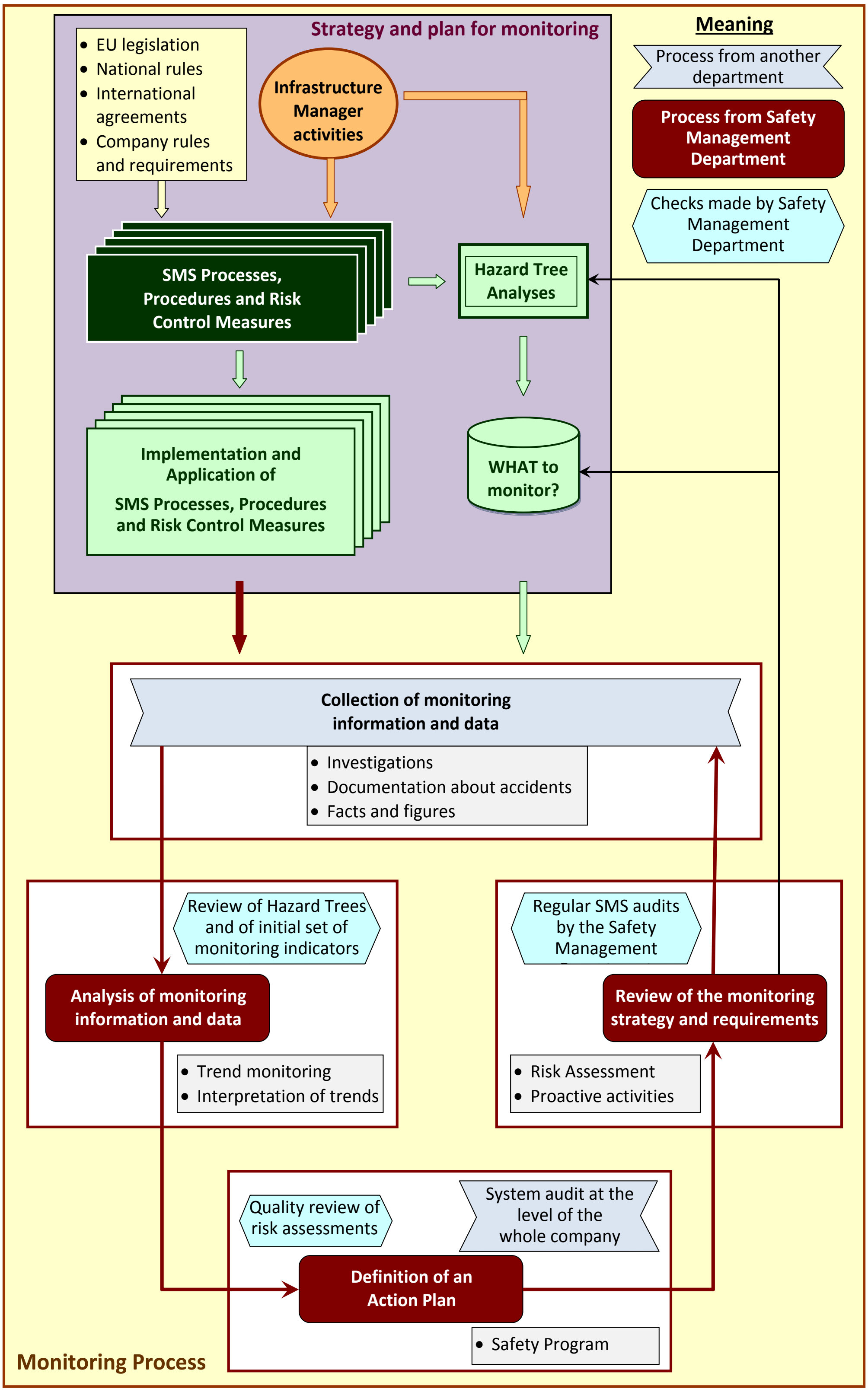


Figure 17: IM strategy for monitoring.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

3.4.3. Collection of information and data

[G 1] In order to monitor the safety performance, every department of the organisational structure of the company, directly or indirectly involved in the operational activities, collects the monitoring information and data defined in the Hazard Tree Analyses for their area of responsibility. For example:

(a) the department for accident investigation is responsible for finding out the (root) causes and the chain of failures that lead to accidents, incidents, near-misses or other dangerous occurrences;

(b) an internal "Rail Net Safety Group" composed of technical experts checks the state of the vehicles that operate on the network;

(c) another "Rail Net Safety Group" composed of operational experts checks the correct application of the SMS processes and procedures by the staff;

(d) the Maintenance Department is responsible for collecting information about maintenance disorders and shortcomings;

(e) etc.

[G 2] All departments communicate the collected information and data to the Safety Management Department.

3.4.4. Analysis of information and data

[G 1] The collected information and data (i.e. facts and figures modelled in the Hazard Tree Analyses) are analysed by the Safety Management Department to measure the actual safety trends in the company.

[G 2] For setting up the threshold values for the indicators to be used for monitoring the safety performance in year Y, the company takes the average values of the corresponding accidents and incidents that occurred during the previous four years (refer to point [G 3] of section § 3.5.6 for an example).

[G 3] A safety expert with a long operational experience registers then the collected information and data into a dedicated database, observes the achieved trends and creates reports concerning either the achievement of the safety performance targets or the degradation of the safety performance in given areas of the company.

3.4.5. Definition of an action plan

[G 1] When the analysis of the collected monitoring information and data reveals non-compliances, all necessary corrective safety measures are taken to restore or to improve the safety performance.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Those safety measures are included in the company Safety Program with a clear description of the reason for their existence as well as the way to implement them.

[G 3] If the corrective safety measures imply a safety relevant change to the infrastructure, the change is analysed before its implementation in compliance with the Regulation on the CSM for risk assessment.

3.4.6. Review of strategy and requirements

[G 1] When non-compliances are detected, in order to ensure there is no forgotten safety measures, the action plan is considered as a change. If the change turns to be significant, it is analysed using the Regulation on CSM for risk assessment. If the change is not significant, a company specific process for risk assessment process is applied to identify clearly all necessary risk control measures.

[G 2] The results of the risk analyses and risk assessments, as well as the documentation for all additional safety measures that were not initially included in the action plan, are collected by the Safety Management Department and taken into account for reviewing the monitoring strategy and requirements. The reviewed monitoring strategy and additional monitoring requirements are then included in the Safety Program of the company.

3.4.7. Evaluation of the safety management system as a whole

3.4.7.1. Introduction

[G 1] Monitoring separately the effectiveness of every process and procedure of the safety management system will show either non-compliance or compliance with the planned outcomes. Although such an approach may require the monitoring of many uncorrelated indicators, checking separately single processes and procedures does not enable the detection of system failures that might lead to the occurrence of accidents, incidents, near-misses or other dangerous occurrences.

[G 2] To verify the effectiveness of the safety management system as a whole, the infra-structure manager makes the following additional checks:

(a) Review of Hazard Trees and of initial set of indicators for monitoring;
(b) Regular SMS audits by the Safety Management Department;
(c) Quality review of risk assessments;
(d) System audit at the level of the whole company.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

3.4.7.2. Review of Hazard Trees and indicators

[G 1] Once a year, an expert panel of the Safety Management Department, under the leadership of a monitoring safety expert, analyses the statistics of the collected indicators from monitoring.

[G 2] A critical review is done to verify:

(a) Is the right indicator defined?
(b) Are other indicators necessary?
(c) Has a safety problem been overlooked? If yes, why did it happen?

[G 3] The outputs[13] from this expert panel are taken as a basis for updating, if necessary, the list of indicators to be monitored.

3.4.7.3. Regular SMS audits by the Safety Management Department

[G 1] Audit experts from the Safety Management Department carry out regular audits (*based on the needs of the Safety Program but more than once a year*) of the correct application of the safety management system. The purpose of the audits is to check the achievement of the objectives defined in the Safety Program of the company. Among others, the audits:

(a) check the correct application of the processes, procedures and risk control measures defined in the safety management system;

(b) check that every department of the company monitors the safety performance of its part of the organisational structure and takes all necessary corrective actions to achieve, and improve where needed, their safety performance;

(c) check the effectiveness of the safety management system as a whole and its appropriateness to achieve the specified safety performance by the company.

[G 2] The non-compliances found out during the audits lead either to actions plans that:

(a) ensure the processes, procedures and risk control measures are correctly applied in the relevant company departments, or;
(b) correct the existing processes, procedures and risk control measures, or;
(c) define additional risk control measures, and;
(d) identify the additional checks to be done during the next audits.

(13) *Possible output from the expert panel: changes of indicators are not needed, or modification of existing indicators or new indicators is necessary.*

3.4.7.4. Quality review of risk assessments

[G 1] Risk Managers from the Safety Management Department perform quality reviews of all risk assessments and risk analyses, i.e. not only of significant changes where the CSM for risk assessment is used.

[G 2] The purpose of these reviews is to ensure consistency in the application of the risk assessment processes and to achieve high quality results.

3.4.7.5. System audit at the level of the whole company

[G 1] In addition to the internal monitoring activities that are scheduled in the Safety Program, other Departments of the company System carry out periodic System Audits of all departments, including the Safety Management Department.

[G 2] This System Audit covers also the safety management system (SMS) and the fulfilment of Regulation (EU) 1169/2010 on the CSM for conformity assessment. All observations and non-compliances identified by the audit are used for refining the monitoring strategy and the Safety Program. That includes the action plan, if needed, with appropriate corrective measures and the lessons learnt for an improved application of the safety management system processes and procedures for the next audit.

3.5. Trend monitoring

3.5.1. Used principle

[G 1] As general approach it is possible to say that catastrophic events are preceded by the occurrence of other events: precursors. If the system is well designed a unique occurrence of a precursor should not lead to a catastrophic event.

[G 2] In the everyday operations, precursors can occur several time, without causing an accident, it means that for a defined number of unwanted events, with no direct impact on the safety performance, one catastrophic damage can occur. If it is possible to detect the precursors, it will be possible to get early warning concerning the behaviour of the system. The monitoring process should be then focused on the precursors, “hidden events” that can help the management to detect a mal-functioning that can lead to poor safety performances. Another way to explain the concept is the “Iceberg principle”.

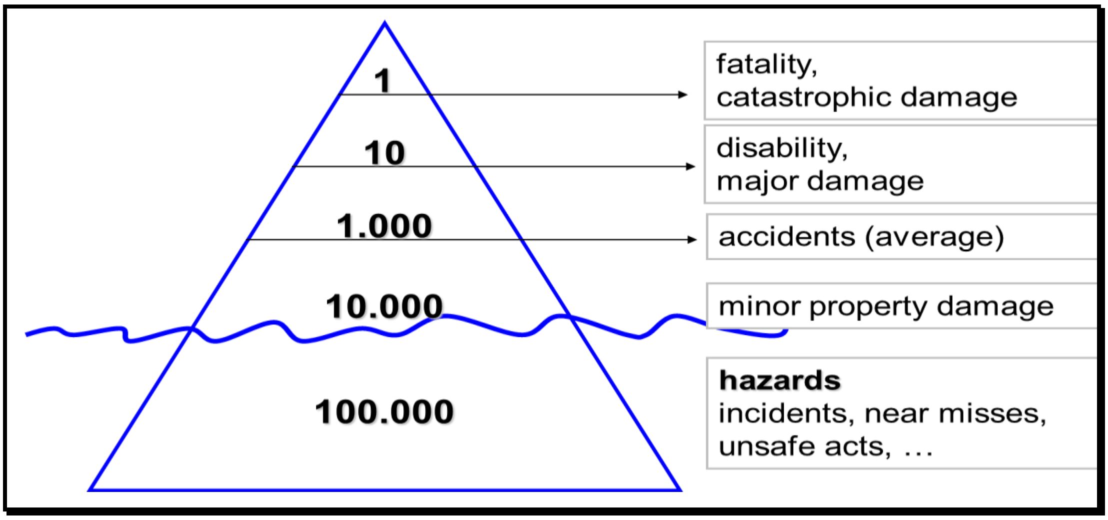


Figure 18: Accidents, incidents, near-misses or other dangerous occurrences identified through Hazard Trees.

[G 3] The "iceberg principle"[(14)] can be applied for monitoring the effectiveness of the safety management system and of its monitoring process which purposes are to:

(a) identify the hazards related to the company activities;
(b) put in place appropriate processes, procedures and risk control measures before the hazards lead to unwanted events;
(c) monitor their correct application and effectiveness;
(d) identify and implement appropriate preventive, corrective or both types of measures if any relevant instance of non- compliance is detected.

[G 4] To achieve those objectives, the monitoring process concentrates the efforts to forecasting and preventing unwanted events such as incidents, unsafe acts and (if they are available) near-misses, including also minor damages caused by an accident, with only material and/or environmental damages, but without human injury or fatality. Detecting early warnings by the monitoring process about potential non-compliances or ineffectiveness of the safety management system enables therefore to prevent accidents with human injuries and/or fatalities.

(14) *The "iceberg principle" is a model that considers not only the visible aspects of a situation but takes into account also the invisible or hidden part. The principle gets its name from the fact that only about 1/10th of an iceberg's mass is seen outside the water while about 9/10th of it is unseen, deep down in water. Consequently, this terminology is used in many (if not most) domains to represent visually that only a very small amount of information is available or visible about a situation or a phenomenon, whereas the "actual" underlying information or bulk of data is either unavailable or hidden.*

[G 5] Experience gained during the application of the monitoring process is used as a learning tool for improving the processes and procedures of the safety management system and increasing the chances to avoid in future more and more incidents and accidents.

3.5.2. Hazards – Input for the monitoring process

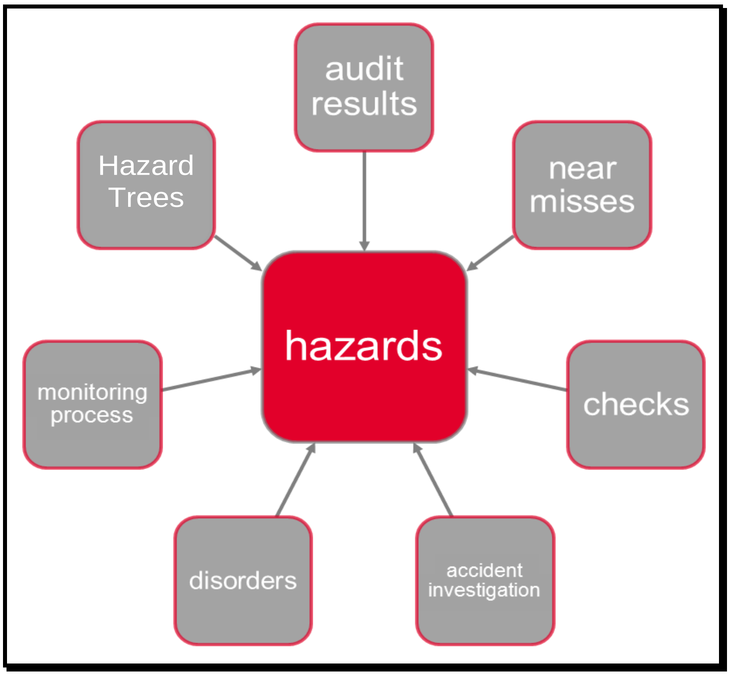


Figure 19: Hazards – Inputs for the monitoring process.

[G 1] As explained in section § 3.4.2, the identification of what to monitor is based on Hazard Tree Analyses built from the risks linked to the infrastructure manager activities. An example of a hazard tree is given in section § 3.5.7.

[G 2] To complete the list of hazards and risks, with the associated indicators, relevant for the monitoring process, the company uses also the following additional inputs (see Figure 19):

(a) all the notes and observations from the audits;

(b) the results of the processing of near misses;
(c) all irregularities from the checks (technical, organisational and operational);
(d) the results from accident investigations with the detailed analysis of the underlying causes and the risk control measures taken immediately, as well as those to be implemented for the future;
(e) the occurrence of disorders and their duration;

(f) the results and trends from the application of the monitoring process and the findings from the observations;
(g) etc.

3.5.3. Modelling of hazards in "Hazard Trees"

[G 1] As explained in section § 3.4.2, the identification of what should be monitored is based on Hazard Tree Analyses built from the risks linked to the infrastructure manager activities. An example of a hazard tree is given in section § 3.5.7.

[G 2] The advantages of using Hazard Trees are:

(a) to model down in a documented and very transparent way the different contributing causes (i.e. underlying hazards) that can lead to an accident, incident, near-miss or other dangerous occurrence;
(b) to build a consistent and clear documentation of all safety related key data;
(c) to show at a glance the relations between accidents and the different underlying causes (hazards) and parameters;
(d) to identify clearly direct links to a possible risk.

[G 3] A Hazard Tree starts with a "top event" (unwanted event) and models down the different contributing causes looking at least for the technical, organisational and operational (human) contributors. The analysis is then extended further to model the accident precursors and as far as possible the root causes for each of these three categories.

[G 4] Let us take as example the "collision" top event: see Figure 20. Let us assume there are 4 collisions and 24 SPADs (signals passed at dangers) per year; many of them are caused by human actions. The modelling of the associated Hazard Tree requires cooperation between the infrastructure manager and the railway undertakings operating on the infrastructure.

(a) the numbers (in red) between brackets are the events and causes which are directly linked to the "top event". In the example, 2 SPADs (hazard or unwanted event) led to a collision; one of these two SPADs was caused by a human;

(b) it is possible that more causes (in this example in level 5) are responsible for one event. So the number of the causes can be higher than the number of the unwanted events/accidents;

(c) level 1 contains the "top event" (i.e. the accident – collision – under analysis). 4 collisions occurred during the observation period;

(d) level 2 models the possible causes of this unwanted top event. SPAD (signal passed at danger) is a possible cause. 24 SPAD’s occurred during the observation period, but only 2 of them led to a collision;

(e) level 3 models down the technical, organisational and human contributing factors that can lead to a SPAD. In the example, only 1 human action directly led to a collision;

(f) level 4 models down the causes of why “a signal can be passed at danger”:

(1) technical causes: which equipment or system failed;
(2) organisational causes: which process or procedure is unclear or wrong, and;
(3) human factors: who made a mistake that led to the analysed event (SPAD). In the example, a driver failure led to a collision;

(g) level 5 represents the fundamental causes (i.e. the mistake or real cause that directly led to the accident) which provoked the collision. In the example, an “inadequate attention at the signal” by the driver led to the collision;

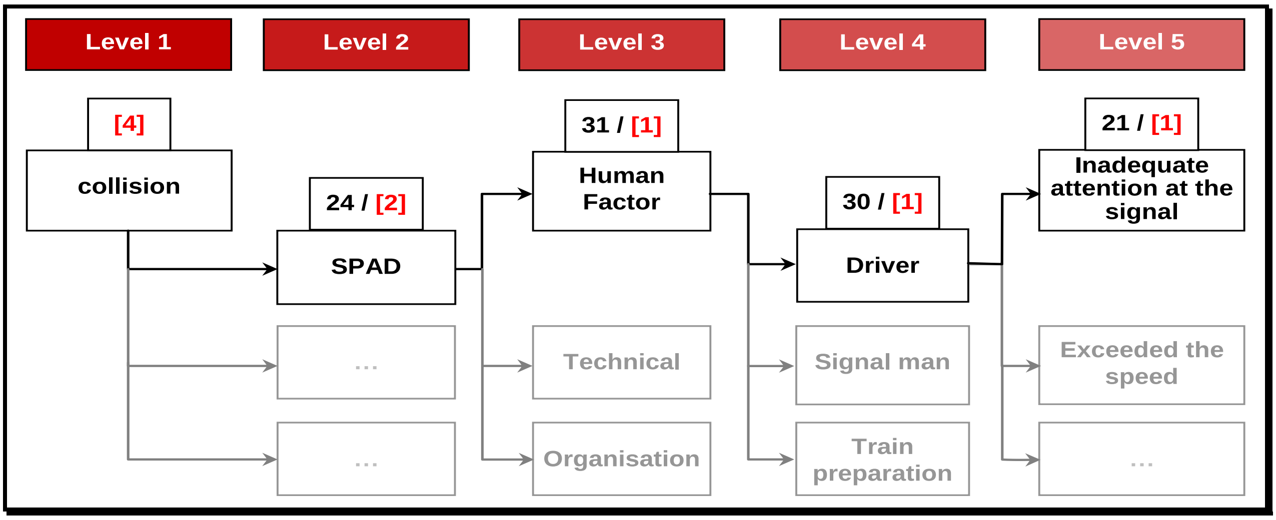


Figure 20: Hazard Tree Analysis for the "collision" top event.

[G 5] In the presented example, it is then important to find out the reasons for the non-compliance. Depending on whether the same driver(s) make(s) many SPADs or whether many drivers make a SPAD at the same signal are different causes of a collision. It is therefore important to determine why some things or some causes have happened. If a negative trend is observed, the coordination between the infrastructure manager and the railway undertaking enables the exchange of the information necessary to control the risks. For the example, it could be necessary to create a joint investigation panel to understand the causes which led the driver not to stop at the right point.

3.5.4. Top Events and identification of indicators to be monitored

[G 1] As explained in the introduction of this example, the identification of the indicators to be monitored is retrieved from Hazard Tree Analyses of the risks that are related to the infrastructure manager activities. Every Hazard Tree starts from a top event, i.e. an accident, an incident, a near-miss or any other dangerous occurrence that the infrastructure manager wants to avoid.

[G 2] A Hazard Tree is built for every of the following types of accidents:

(a) **train collision**: it analyses the causes of the *"train to train, train to obstacle, train to shunting unit, train to a track closure"* collisions;

(b) **train derailment**: it analyses the causes of all derailments of trains;

(c) **shunting accidents**: it analyses the causes of the *"shunting unit to shunting unit, shunting unit to obstacle, shunting unit to a track closure"* collisions, the shunting derailments, the rolling away of vehicles, and other (smaller) shunting accidents and incidents;

(d) **other accidents**: it analyses the causes of all other types of accidents (except the train or shunting accidents listed in previous three points) and the accidents in some specific modes of operation;

(e) **level crossing accidents**: it analyses the causes of all accidents, incidents, near-misses or any other dangerous occurrence at secured and non-secured level crossings between "a train or a shunting unit" and "a road user";

(f) **disorders and shortcomings**: it analyses the relations/interactions between accidents, incidents, near-misses or any other dangerous occurrence and the staff non-compliances with the processes and procedures of the safety management system;

(g) **injuries and fatalities**: it analyses the causes of injuries and fatalities.

[G 3] All the indicators to be monitored by the different departments of the infrastructure manager are derived from those Hazard Trees which model down all identified causes of accidents, incidents, near-misses or any other dangerous occurrence. The indicators are used to take corrective or preventive actions at the earliest possible stage before the hazards result in accidents, incidents, near-misses or other dangerous occurrences.

3.5.5. Company safety targets

[G 1] Basically, the company safety targets are defined based on international requirements, European legislation and national rules: see Figure 21. They are inputs also for setting up the company safety performance requirements and the safety performance for every department of the company.

[G 2] The top management is committed to safety. It lays down the company safety paths and safety policy for every year. The importance of safety for the daily business of the infrastructure manager is clearly communicated to the employees in a safety mission statement. Based on the experience of the previous year, the top management reviews every year the company safety targets.

[G 3] Every month, the Safety Manager, in coordination with the different departments of the company, reports to the top management, about the achievement of the safety performance and safety targets.

[G 4] The monitoring process is the key instrument for managing the achievement of the safety performance and safety targets. It is a proactive tool for collecting indicators and identifying as early as possible deviations from the expected safety performance so that corrective/preventive actions can be taken sufficiently in advance before accidents, incidents, near-misses or other dangerous occurrences happen.

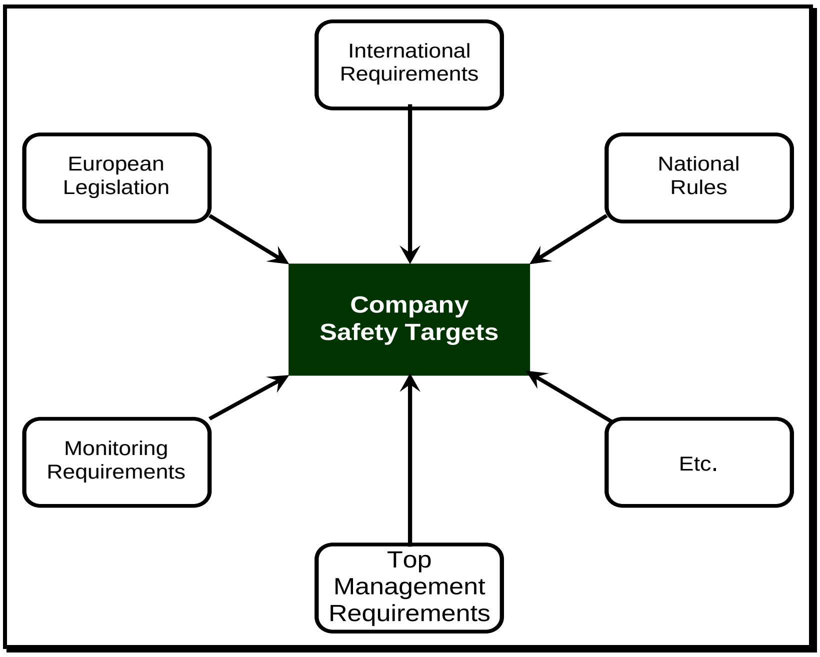


Figure 21: Company safety targets.

3.5.6. Signal function or alarm function

[G 1] The infrastructure manager uses an internal IT-tool, called "signal function". This IT-tool is used for calculating the thresholds of safety critical indicators of the company (called also "key performance indicators"). The algorithm of the IT-tool is based on one side on recital 4 of the safety Directive 2004/49/EC:

Safety levels in the Community rail system are generally high, in particular compared to road transport. It is important that safety is at the very least maintained during the current restructuring phase, which will separate functions of previously integrated railway companies and move the railway sector further from self-regulation to public regulation. In line with technical and scientific progress, safety should be further improved, when reasonably practicable and taking into account the competitiveness of the rail transport mode.

[G 2] On the other side, the algorithm of this IT-tool is also based on the method to calculate the common safety targets (CST).

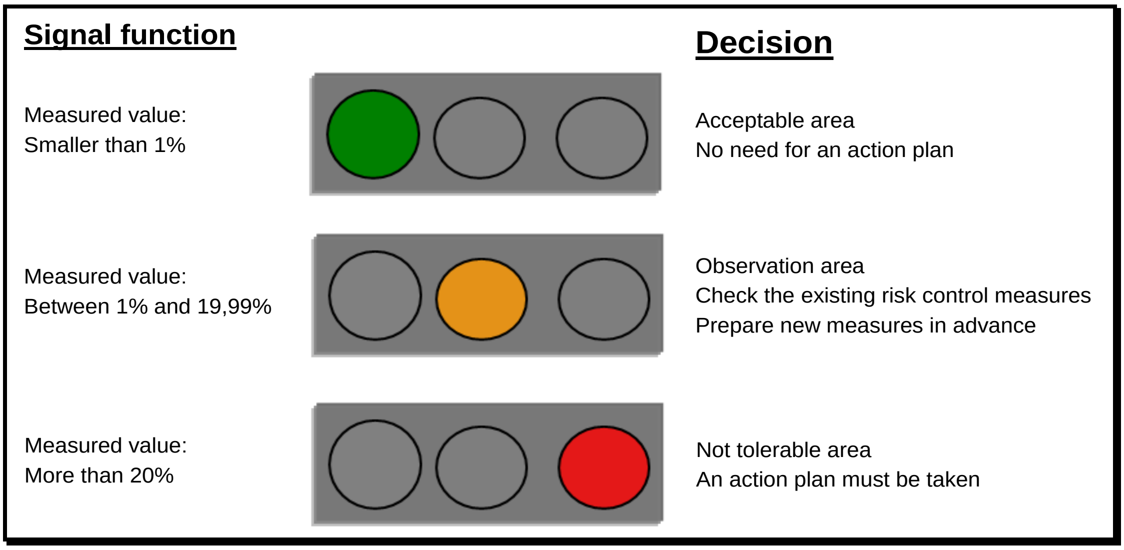


Figure 22: Signal/alarm function for key performance indicators.

[G 3] For the safety performance targets of the 2010 year, the company took as threshold values the average of all accidents that occurred during the previous 4 years, i.e. from 2006 to 2009. Based on that in 2011, the top management set up long-term safety performance targets that should be achieved by the year 2025. This long term objectives led to define requirements for an annual improvement of the safety performance.

[G 4] To follow the tendency of the safety performance in relation to the increase or decrease of business within the company, it is necessary to take into account the average of the train*kilometres in the analysed period.

This "kilometre average" is a multiplying factor in the algorithm. It is setup at "1", but:

(a) if during the analysed period more train*kilometres are run, the multiplying factor is setup higher than "1";

(b) if during the analysed period less train*kilometres are run, the multiplying factor is setup smaller than "1".

[G 5] Consequently, the measurement of the achieved safety performance is a combination of the number of reported indicators[(15)] and the train*kilometre average. The top management uses also this "signal function measurement" to set up the thresholds for the safety critical indicators.

[G 6] The Safety Management Department reports to the top management on a monthly basis the measurement of the safety critical indicators with this "signal function" IT-tool.

3.5.7. Example of a "hazard tree": "train collision" with signal function

[G 1] The example of a hazard tree for a "train collision" is shown in Figure 23.

[G 2] Figure 23 is an example of how the infrastructure manager models in a Hazard Tree the causes that can lead to a considered "top event".

[G 3] For every unwanted top event (critical indicators), there is a programmed "signal/alarm function" in the supporting IT-tool with a threshold value. This feature enables to see at a glance the company risks and to define preventive risk control measures in the Safety Program before the top event actually happens.

(15) *Reported indicators are related to accidents, incidents, near-misses or any other dangerous occurrence, including all the top events listed in point* ***Error! Reference source not found.*** *of section* ***Error! Reference source not found.***.

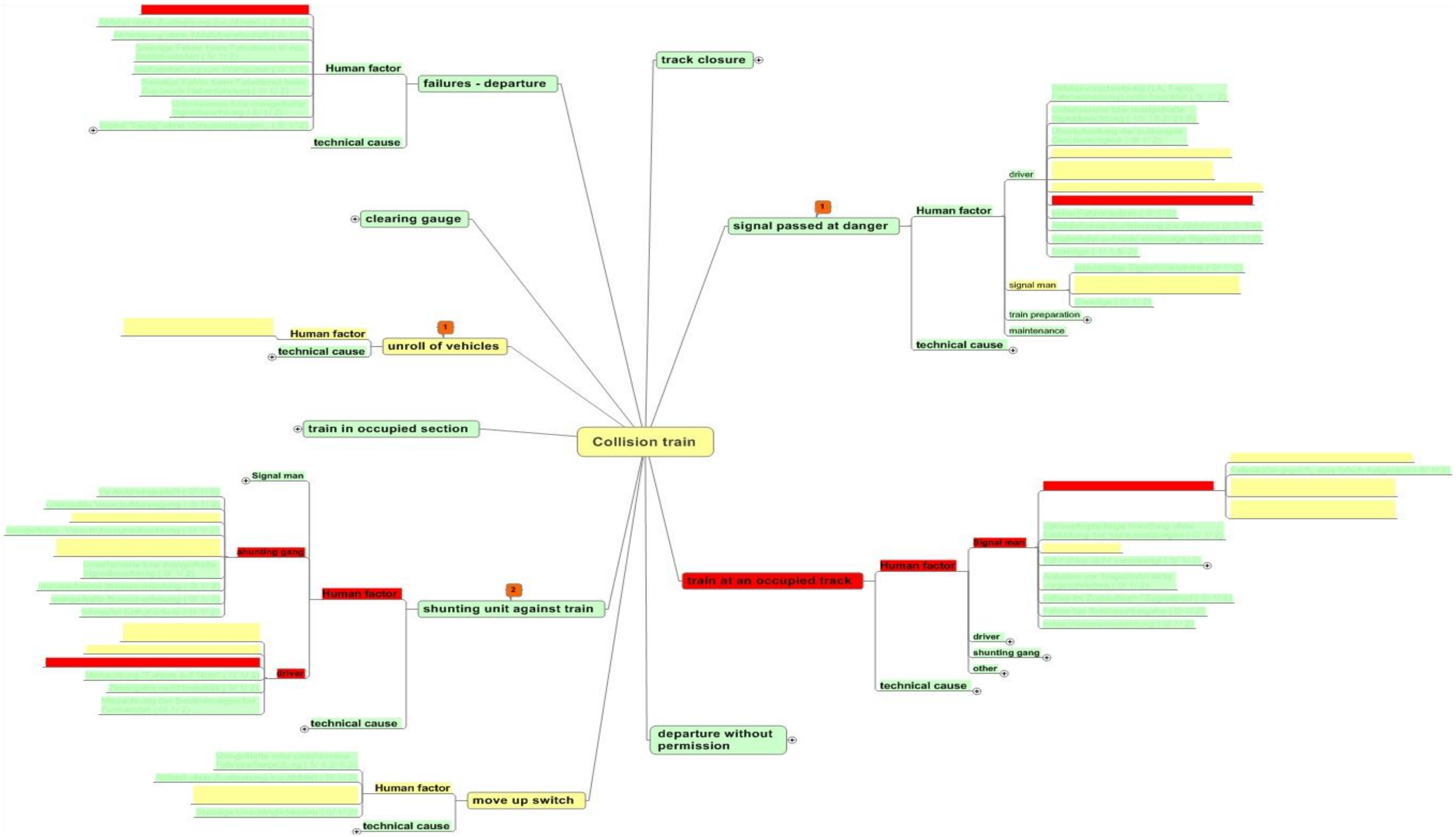


Figure 23: Example of a "hazard tree": "train collision" with the "signal/alarm function".

3.6. Safety Program (action plan) – Set up and update

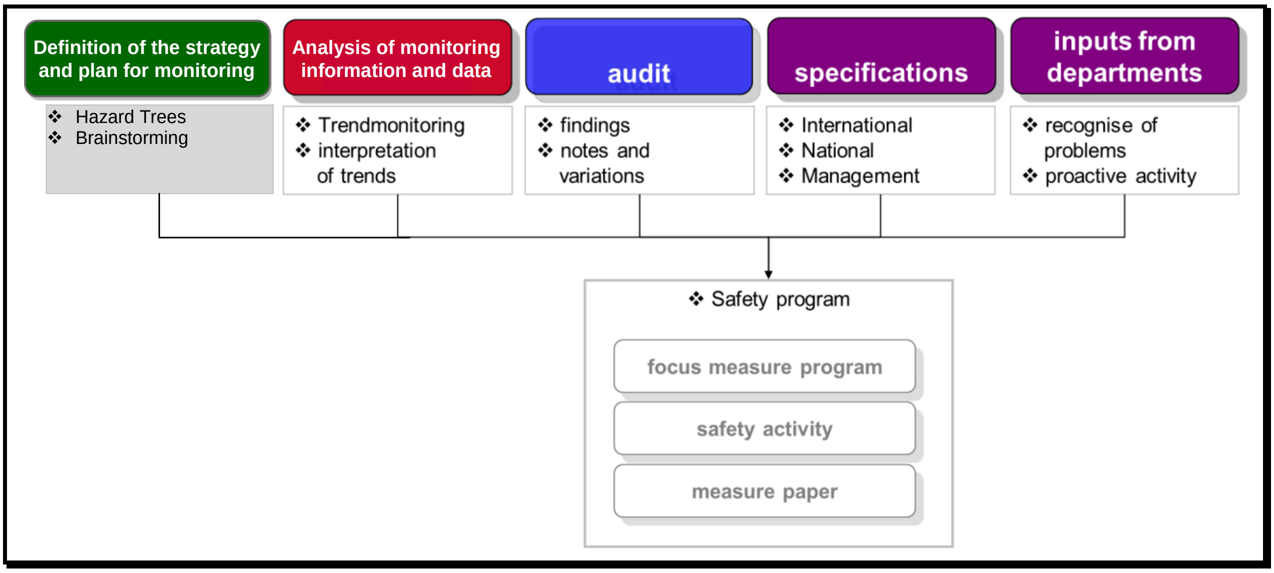


Figure 24: Inputs of the Safety Program.

[G 1] Different inputs are used for setting up and updating the Safety Program (see Figure 24):

(a) the Safety Program is initially populated with the results of the Hazard Tree Analyses. It includes the indicators that are to be monitored: refer to section § 3.4.2;

(b) then, based on the application of the different processes and procedures of the safety management system, as well as on the results collected through the monitoring process, additional inputs are made available. They are used to review the initial set of indicators for the monitoring activities. These additional inputs to the Safety Program include the measures and associated indicators:

(1) for correcting the non-compliance detected by the "trend monitoring" that shown a tendency to decrease the safety performance;

(2) for addressing all findings, notes and variations discovered during internal and external audits. In this case, the corrective measures are also taken into account for the continuous improvement of the company safety management system;

(3) if necessary, for implementing (new) international or national regulations, or new specifications from the top management;

(4) if defined by any department of the company either for correcting the detected non-compliances or for putting in place preventive measures necessary to continue maintaining or to improve their safety performance.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] After the identification of the need for an action plan (i.e. for corrective or additional risk control measures), three possibilities exist in the Safety Program:

(a) 1st – large scale measure;
(b) 2nd – safety action;
(c) 3rd – documentary measure

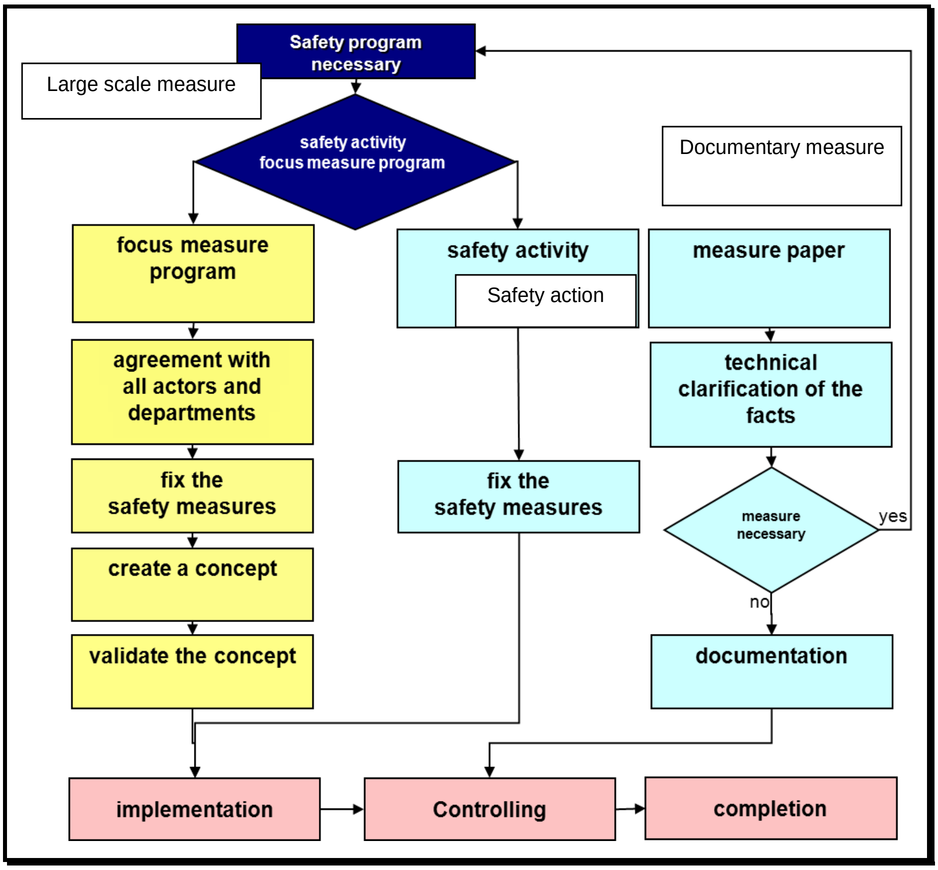


Figure 25: Decisions for the Safety Program.

[G 3] When the need for an action plan is identified, the following question has to be answered: “Is a large scale measure necessary or is a safety action sufficient?”

(a) a **large scale measure** is an action plan with a high cost (i.e. very expensive risk control measures), when more than one department is impacted or when a big safety related infrastructure improvement is necessary (e.g. fitting a line with ETCS).

For a large scale measure, an agreement of all managers from the affected departments is necessary. This group of managers decides on the risk control measures to put in place and creates a concept paper. This concept paper is submitted to validation (i.e. to authorisation) from the headquarter operational department.

(b) a **safety action** is an action plan with limited number of risk control measures and usually with reasonable costs. In most of the cases, this happens when a department needs to adopt preventive or corrective measures to manage a non-compliance.

(c) a third case is a **documentary measure**. This might require a documentary justification of the observed facts and measured figures when looking at the safety performance tendency during the "trend monitoring". Based on the documentary justifications:

(1) if deemed necessary, it can be decided to put in place additional risk control measures. In this case, there will be a "safety action" through the management of the Safety Program, or;

(2) if the justifications are sufficient, the decision is that no measures are necessary. But, the observed non-compliances are submitted to special attention during the "trend monitoring" of the next period (at least 6 months later).

[G 4] The management of the action plan implementation is the same for all three cases:

(a) the risk control measures defined in the action plan are implemented;
(b) the effectiveness of the action plan is verified through the application of the monitoring process for the new risk control measures and associated indicators;
(c) the activities are documented in compliance with the procedures of the safety management system.

3.7. Safety key performance indicator (KPI)

[G 1] The safety key performance indicator is a report with key figures about the development of the overall safety performance. The report is communicated to the top management on a monthly basis. It is also made available to all the employees.

[G 2] In the daily business, the infrastructure manager is monitoring about 1.500 safety related indicators. They were identified through the 7 Hazard Trees. The defined events for the Key Performance Indicator are (Figure 27):

(a) train collisions;
(b) train derailments;
(c) collision with track closure;
(d) level crossing accidents, collision with obstacles;
(e) Shunting accidents:

(1) Shunting collision;
(2) Shunting derailment;

(f) Human failures (incidents).

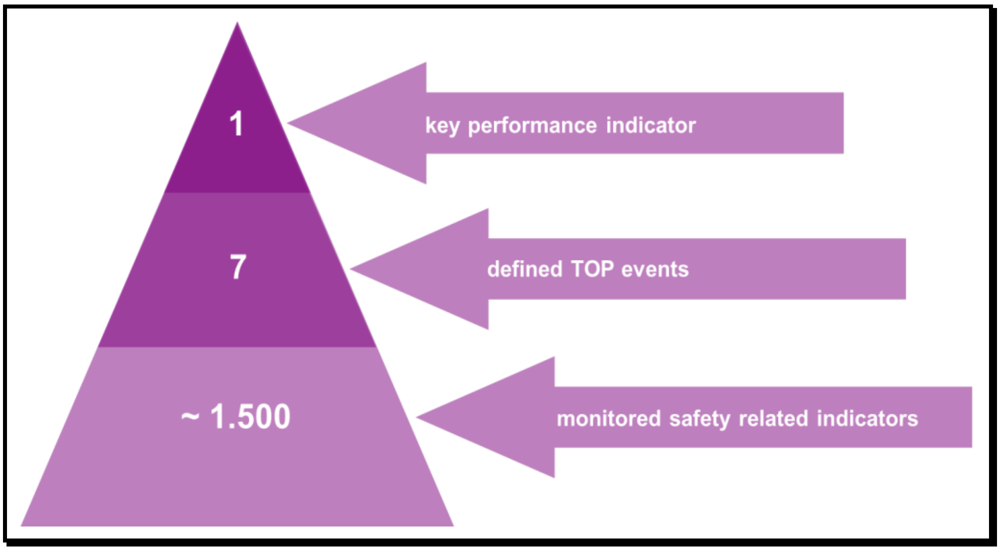


Figure 26: Key performance indicators.

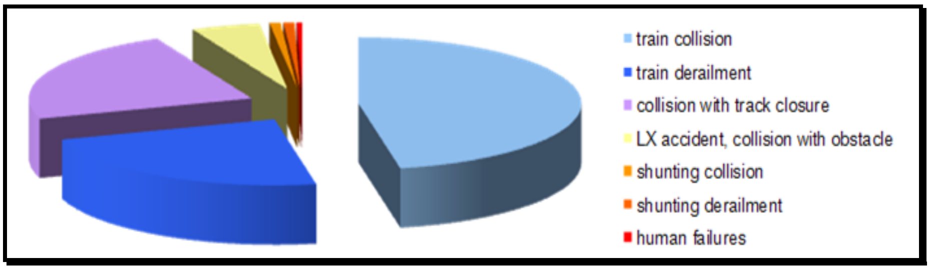


Figure 27: Unwanted events, accidents and unsafe acts.

[G 3] Based on the collected monitoring information and data, an expert panel assesses these top events. To determine the relative value for the associated key performance indicator, the expert panels weights the top events taking into account, on one hand, the severity of the associated accident and, on the other hand, the run train*kilometres. To get a smoothed value, one point on the diagram is always the combination of the summed weighted events over 12 months and the 12 month average of the train*kilometres.

[G 4] Two key performance indicators (KPI) are reported monthly:

(a) 1st : the KPI for the whole network safety performance. It represents all values of the defined indicators caused by all the actors in the whole railway system of the infrastructure manager. This KPI includes therefore also the accidents caused by the railway undertaking that operate on the network;

(b) 2nd : the KPI for the infrastructure manager alone. It represents the safety performance measured through the indicators related purely to the infra-structure manager activities.

[G 5] Figure 28 represents an example of the evolution of the tendency of a key performance indicator:

(a) the red line with breakpoints represents the measured values for the considered safety key performance indicator.

The indicator is measured every month. It is reported by a point on the diagram. The value of the indicator is the product between the summed and weighted top events over 12 months and the 12 month average of the train*kilometres. That way of calculating permits to distinguish random occurrences of the considered top events and systematic failures;

(b) the black dotted line represents the tendency of the KPI calculated linearly;

(c) the green upper line represents the acceptable area. If the measured KPI is located in the green area (i.e. bellow the upper straight green line) the achieved safety performance is compliant with the safety targets set up by the company top management.

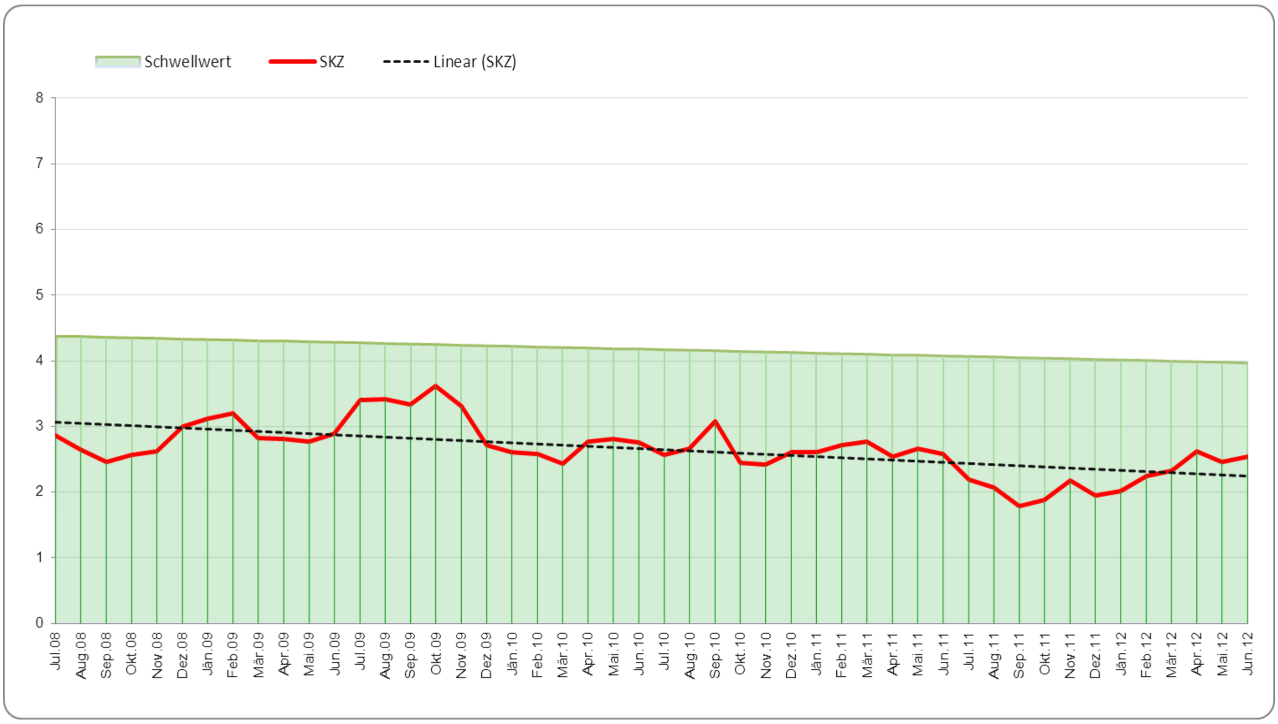


Figure 28: Key Performance Indicators (KPI).

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

4. Example 4: Monitoring by a Railway Undertaking

4.1. Context of the example

Table 33: Monitoring by a Railway Undertaking.

Kind of railway actor	Railway undertaking
Articles and/or sections in the Annex of Regulation 1078/2012 that the example most closely relates to	The example is mainly connected to article 3.2(a) and section 2 in the annex of Regulation 1078/2012. Although the considered railway undertaking uses other methods for identifying exhaustively the items to monitor, the example focuses only on the "hierarchical check" part to show how the *"definition of a strategy and priorities for monitoring"* can be done.
Description of the example, including among others: • its scope; • how it fits within the overall monitoring framework; • a brief summary of the content; • any limitations: *all process steps are not shown, all details of the process step are not presented; only examples are shown, etc.;* • who uses the example; • other relevant information	This example is based on the return from experience of a very big European Union railway undertaking that acts in the following fields: "freight transport, passenger transport, driving services, supply and maintenance of rolling stock, services related to infrastructure, etc." The example describes briefly how a monitoring strategy can be elaborated by the top management of a company based on the structural organisation of the company. The level of details documented in this guideline is intentionally low as the *"definition of a monitoring strategy"* is strongly dependent on the size and structural organisation of every company as well as on the services the company provides. The *"definition of the monitoring strategy"* in the present example is also linked to the Safety Policy described in the safety management system of the company. The example focuses only on the "hierarchical checks" that can be implemented to detect failures of the company staff to comply with the mandatory safety requirements(16) in the safety management system. The use of hierarchical checks is only one part of the monitoring strategy in the company. Indeed, hierarchical checks are one of possible ways for monitoring the safety level in a company by involving directly the management resources. Any company that monitors activities related to safety could use hierarchical checks in association, or not, with other tools such as information of return from experience, audits, inspections, etc. The used combination of these tools is defined in the monitoring strategy.
How could it be used by other actors?	The concepts described in this example could be used by other companies. However they must be adapted to the structural organisation and specificities of the activities and SMS of every company.

(16) *Mandatory safety requirements are included in the safety management system of the company. They can include internal company rules, requirements from European or national legislation or constraints from international agreements.*

4.2. Introduction

[G 1] Although the example illustrates how a railway undertaking can identify the indicators to be used for monitoring the safety performance of its activities, it is pointed out that:

(a) the definition of the indicators must be adapted to the specificities of every company and the particularities of its SMS. The company organisation, operation, processes, tasks, company management, etc. are different from company to company. All those company characteristics condition the indicators to be used for monitoring the safety performance of its safety management system;

(b) the example is not exhaustive. The indicators cannot be copied and pasted. The example illustrates nevertheless how the indicators can be defined in an exhaustive and systematic way;

(c) the methodology used in the example is not the only possible approach to define indicators. Other ways of identifying indicators is also possible.

4.3. Definition of a strategy for monitoring

4.3.1. Introduction

[G 1] The monitoring strategy describes how the company actively controls its safety level. It is derived from the Safety Policy of the company. It is based on a proactive approach that enables the company to detect non-compliances at an early stage and to take corrective and/or preventive measures before the detected non-compliance escalates into an accident, incident, near-miss or other dangerous occurrence. In addition to that, the detected non-compliances are analysed in order to find out their causes and improve the safety management system of the company.

[G 2] To define the monitoring strategy, the company looked at the following questions:

(a) Q 1: What shall be monitored?
(b) Q 2: Who is responsible for the items to be monitored?
(c) Q 3: Which methods to use for monitoring what is to be monitored?
(d) Q 4: How is the monitoring to be managed?

4.3.2. Scope of the monitoring and responsibilities

[G 1] This section answers the first two questions:

(a) Q 1: What shall be monitored?
(b) Q 2: Who is responsible for the items to be monitored?

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] To identify the items/actions to be monitored, the company makes first the inventory of all the activities related to safety in the different parts of the company taking into account the main interfaces between those different parts of the company.

[G 3] The company considers ***as related to safety*** *"all activities, whatever their nature is (design, implementation, operation, maintenance), which when they are performed by a person or an entity they generate risks for people or equipment during operation of the railway system".*

[G 4] The inventory of the activities related to safety takes into account all the services delivered by the company: freight transport, passenger transport, driving services, supply and maintenance of rolling stock, services related to the infrastructure, etc.

[G 5] Every activity related to safety is then characterised by:

(a) the description of the set of elementary tasks (i.e. necessary technical equipment, processes to apply, actions to be performed by human operators, etc.) necessary to be fulfilled for delivering the considered services;
(b) the description of who is in charge of executing every elementary task.

[G 6] For example, Table 34 shows the set of elementary tasks to be fulfilled to deliver the "freight transport activity".

Table 34: Set of elementary tasks for delivering the freight transport activity.

Elementary tasks	Task executed by the Activity itself	Task executed by somebody else
1 Resources management for the offer and design of services		
1.1 Projects for new systems: set of the documentation	X	Partially
1.2 Request of access to operate on a network of another Member State: application for Safety Certificate Parts B	X	
1.3 Path demands	X	Partially
1.4 Managers' training	X	
1.5 Subcontractor's contracts management	X	
…		
2 Driving, shunting and running of trains		
2.1 Selection, training and certification of operators	X	Partially
2.2 Use of shunting locomotives	X	
2.3 Verification of train before accessing the network	X	
…		
3 Safety management system		
3.1 Management of safety documents	X	
3.2 Investigations and collection of feedback	X	
3.3 Information to be given in case of accident/incident	X	
3.4 Management of safety when using contractors	X	
…		

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 7] For example, Table 35 shows the set of elementary tasks to be fulfilled to deliver the "activities at stations".

Table 35: Set of elementary tasks for delivering the activities at stations.

Elementary tasks	Task executed by the Activity itself	Task executed by somebody else
1 Stations development, improvement and maintenance		
1.1 Definition of the operating program	X	
1.2 Granting and renting of spaces	X	
…		
2 Operating of the stations		
2.1 Set of the general working rules of a passenger station	X	
2.2 Definition of the interface rules between the IM and RUs	X	
2.3 Passenger information		X
2.4 Taking of persons with reduced mobility (PRM)		X
…		
3 Safety management		
3.1 Setting of safety targets	X	
3.2 Management safety documents	X	Partially
…		

4.3.3. Identification of the items/actions to monitor in an elementary task

[G 1] As described in point [G 5] of section 4.3.2, every activity is composed of a set of elementary tasks executed by a number of people in the organisational structure of the company. And every elementary task can be composed of a set of actions or items.

[G 2] Every person responsible for the execution of an elementary task in a safety related activity has to identify the scope of its monitoring responsibilities:

(a) the identification of the items/actions to monitor must be exhaustive as far as possible because all items/actions related to safety are to be monitored within a given time period (e.g. between 3 months and 3 years, depending on the nature of the considered item or of the responsible person);

(b) priorities for monitoring are to be set up based on the level of criticality of every item/action and included in the Monitoring Plan of the company.

[G 3] The identification of those critical items/actions in every elementary task and the setting up of the monitoring priorities can be done using the following methods:

(a) **Brainstorming:** a manager leads the reflection with the concerned operators taking into account the results of accident/incident investigations, the analysis of the return of experience, the review of the documentation, the actions to be performed by human operators (e.g. working instructions), etc.

(b) **Risk assessment:** applying appropriate risk assessment tools a risk assessment expert identifies for every elementary task:

(1) the risks and the related causes;
(2) the associated items/actions that are to be monitored in order to verify the compliance with the safety performance requirements planned in the safety management system.

Using risk priority numbers, this method allows then the quantification and classification of the items/actions to be monitored.

(c) **Continuous follow up of the triggering events:** this method is based on the return of experience where some events in the past triggered an accident, incident, near-miss or another dangerous occurrence.

Remark: It is must be underlined that this method cannot be used alone. It is a reactive approach that enables to protect only against those hazards and risks that caused the same unwanted events in the past.

4.4. Tools for monitoring – Hierarchical checks

4.4.1. General

[G 1] This section answers the question **"Q 3: Which methods to use for monitoring what is to be monitored?"**

[G 2] Several methods or tools can be used, alone or in combination between them, to monitor the items/actions identified in section § 4.3.3.

[G 3] Although other methods are used by the considered railway undertaking, the present example illustrates only the hierarchical checks. It is the main company method for monitoring the compliance with the prescriptions of the safety management system. It allows the systematic monitoring and within an appropriate periodicity of all the "critical" items/actions related to safety.

[G 4] The hierarchical checks, typically a function of the management, enable to comply with Regulation N°1078/2012. They enable to:

(a) measure the level of the achieved safety performance by the company;
(b) analyse the collected monitoring information;
(c) compare the obtained results to the requirements specified in the safety management system and verify whether there are non-compliances with the requirements;

(d) in case non-compliances are detected, identify and implement appropriate preventive and/or corrective measures through an action plan;
(e) review the impact of the action plan on the monitoring strategy, priorities and plan(s) for improving the safety management system of the company.

[G 5] Hierarchical checks are performed by every manager of the organisational structure of the company that is under its responsibility. The objective is:

(a) to check the correct application of the safety management system processes and procedures;
(b) to check both in normal and in degraded situations whether the detected deviations are:
    (1) occasional, i.e. isolated or occurring from time to time;
    (2) repetitive, I.e. occurring on a regular basis;
    (3) individual, i.e. executed systematically by the same persons;
    (4) collective, i.e. affecting more than a few persons.

[G 6] The hierarchical checks cover:

(a) the operators or team work: competences, skills, training, etc.;
(b) the organisation: appropriateness to the needs, with a particular care to the interfaces;
(c) the procedures: their existence is fully justified, conformity of the understanding with the requirements, structure, readability and comprehensibility of the documentation, etc.;
(d) the equipment and tools: ergonomics of the work station, etc.;
(e) the work environment;
(f) the safety for the passengers, the third parties or the goods.

[G 7] The verification of the operators and of the items/actions that are carried out by those operators allows the hierarchical checks to get a better knowledge of the part of the railway system for which the company is responsible.

4.4.2. Levels of hierarchical checks

[G 1] Hierarchical check are done at the following two levels of the company:

(a) **level 1:** the company being composed of a number of different entities, "every entity manager" is in charge to organise and lead the hierarchical checks for its area of responsibility. The entity manager and the local managers perform the necessary checks and capitalise on the results. They elaborate the appropriate action plans taking into account the results of these hierarchical checks;

(b) **level 2:** the "entity director" is in charge to manage also hierarchical checks at the system level. The purpose is to enable the evaluation of the quality management of the safety that is performed by the local entities.

This level of hierarchical checks allows the "entity director" to verify that the different "entity managers" permanently survey the safety level of their entity, detect on time any deviation from the requirements and undertake all necessary corrective actions. To this end, the entity director follows the progress of the implementation of the actions plans and measures their effectiveness.

[G 2] The "level 1 hierarchical checks" consist mainly in:

(a) checking the operators in their working conditions and environment;
(b) analysing the safety documentation;
(c) inspecting the equipment and tools directly linked to the safety;
(d) verifying the quality of safety management done by the local managers.

[G 3] The "level 2 hierarchical checks" consists mainly in:

(a) checking the control of the safety processes is done in every entity;
(b) checking the conformity of the equipment and the working environment;
(c) checking the interfaces management;
(d) checking the quality and the effectiveness of the safety management for which the entity managers are responsible.

[G 4] The number and the nature of hierarchical checks are determined with realism based on expert judgement. The identification of the items/actions to be monitored through hierarchical checks (refer to section § 4.3.3) takes care they are relevant and sufficiently representative to enable not only the detection of non-compliances but to give early warnings about possible deviations that may result in a non-compliance or in a situation with potential risks.

4.4.3. Types of hierarchical checks

4.4.3.1. Introduction

[G 1] Several types of hierarchical checks can be used depending on the item/action to be monitored:

(a) A priori checks (or offline checks);
(b) Checks on the field (or field audits);
(c) A posteriori checks (or cross checks);
(d) Checks of the safety management;
(e) Watch plan (or vigilance plan);

[G 2] That list is not exhaustive.

4.4.3.2. A priori checks (or offline checks)

[G 1] The purpose of "a prior checks" is to verify that the operators in charge of safety related tasks have all necessary resources and competences, equipment and tools for performing correctly their tasks.

[G 2] "A priori checks" verify the following:

(a) the adequacy between the organisation and the tasks that are planned;
(b) the documentation relevant for the task is updated, accessible to the staff, etc.;
(c) the training and certification are planned;
(d) the state of the necessary equipment and tools.

4.4.3.3. Checks on the field (or field audits)

[G 1] The "checks on the field" consist in observing the operators directly at their work place and environment. They enable to verify that:

(a) the operators know and understand the applicable regulations and requirements;
(b) the operators uses the appropriate equipment and tools but also know how to use them;
(c) the operators use the appropriate procedures and know how to apply them (know-how), and;
(d) the operators adapt their behaviour to the situations (inter-personal skills).

4.4.3.4. A posteriori checks (or cross checks)

[G 1] The purpose of "a posteriori checks" is to cross-check all the available sources of monitoring information to verify that every procedure and every parameter of a designed procedure or of a product is appropriate and enables to comply with all applicable regulations and requirements.

[G 2] They can be applied to written procedures, review of recordings or state of a product, equipment or tool.

[G 3] The "a posteriori checks" enable to verify the correctness of the control of the formal procedures, the control of the use of equipment and tools and the quality of the human behaviour, in particular concerning radio communications.

4.4.3.5. Checks of the safety management

[G 1] The check of the safety management include:

(a) interviews of managers and their deputies;
(b) analysis of the organisational structure of the teams;

(c) verification of how the annual objectives allocated to managers are taken into account in performing their work;
(d) examination of the watch/vigilance plans;
(e) review of the progress in implementing the agreed action plans;
(f) sample checks of methods applied by the "level 1 hierarchical checks";
(g) analysis of the feedback and return of experience data;
(h) etc.

4.4.3.6. Watch plan (or vigilance plan)

[G 1] The watch plan is an iterative tool which contains the description of the staff tasks, the processes to be checked and the results expected to be observed from those checks. Every level manager (i.e. the local managers, the every entity manager and the entity director) creates its own watch plan and uses it as a tool for manage actively the safety.

[G 2] The purpose of a watch plan is to:

(a) allow an analysis of each process and employee in order to identify potential non-compliances (called weak points in that company);
(b) check the completeness of the checks at the different levels of the organisational structure of the company;
(c) contribute to the setting up of necessary action plans for correcting or mitigating the detected non-compliances (called weak points in that company);.

[G 3] The watch plans are built so that a simple reading directly points out the strong and weak points of the items/actions that are in the scope of the hierarchical checks. These items/actions can concern the operators, the procedures, the equipment, the organisation and the environment.

[G 4] For this reason, the data collected in a watch plan have a clear classification. The classification depends on the nature of the non-compliance taking into account its context in terms of risk and its severity. An example of classification is shown in Table 36:

[G 5] The analysis of the data collected in a watch plan enables to define and implement the necessary corrective actions.

[G 6] The watch plan is a picture of the level of safety of an entity and allows the detection of violation of alert thresholds. It is a living plan which takes into account each modification or event that could have an impact on the items/actions that are monitored.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table 36: Classification of non-compliances in a watch plan.

Classification	Meaning
Good	No deviation
Acceptable	Minor deviation
Poor	Deviation that has an impact on the global safety level but without any direct consequences on the safety. It is a significant deviation in comparison with all applicable standards, regulations and requirements.
Not acceptable	Critical state that can have a direct impact on the safety. The requirements are not fulfilled and there is no control of risk

Table 37: Example of a watch plan for the "Head of Traffic Department"/Signalman tasks.

Competence management plan				From	####	To	####					
Role:	Head of Traffic Department			N. of controls displayed:			3					
				Agent								
ID	Macro competence	Competence	Micro competence	CAI			GCX			ACI		
S0	Generalities	Qualification	Requirement: Psycho-Physical Attitude			S		S	S			S
			Requirement: other than Psycho-Physical Attitude									
		Knowledge of the hand-books	Signatures to trace the distribution of handbooks	I	I	A	S	I	S	I	I	A
			Real knowledge of the handbooks	I	S	S	S	S	S	I	S	S
		Begin / End of service	Beginning of the service			NC	S	S	S			NC
			Handover with the next worker in shift			NC	S	S	S			NC
		Safety com-munication	Use of radio during shunting	S	S	S	S	S	S	S	S	S
			Exchange of dispatches			NC	S	S	S			NC

[G 7] Table 37 shows an example of structure of a watch plan for the "head of traffic department"/signalman. It can be used to follow up the operators' tasks, where:

(a) on the left hand side of the table, all safety related activities of the operator are listed for the given safety job (here signalman);

(b) on the right hand side of the table, each operator (quoted as CAI, GCX,…) of the entity concerned by this job is followed up.

Then a classification as presented in Table 36 is used.

4.4.4. Processing of information collected through hierarchical checks

4.4.4.1. Introduction

[G 1] This section describes the way to use the results of the hierarchical checks. Among others, the following needs to be done:

(a) Recording of information collected through hierarchical checks;
(b) Correction of non-compliances (i.e. deviations);
(c) Overall corrective actions;
(d) Validation of corrective actions.

[G 2] This list is not exhaustive.

4.4.4.2. Recording of information collected through hierarchical checks

[G 1] The recording of the information collected by the hierarchical steps is essential. It provides a documented traceability between the non-compliances detected by the different hierarchical check levels, the necessary corrective actions and the validation of the effectiveness of the proposed corrective actions.

[G 2] The traceability of information from hierarchical check can also be used in case of juridical enquiry against the company to demonstrate that the company did all what was reasonable feasible to manage safely its operations.

4.4.4.3. Correction of non-compliances (i.e. deviations)

[G 1] An analysis of the causes, and as far as possible of the root causes, is done in order to:

(a) identify the reasons for the non-compliance;
(b) define and implement the appropriate corrective actions.

4.4.4.4. Overall corrective actions

[G 1] Non-compliances in the staff knowledge or non-compliances in the staff behaviour can lead either directly or in combination with other failures to an accident, incident, near-miss or other dangerous occurrence. When hierarchical checks reveal such non-compliances, the following measures are necessary:

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) individual or collective interviews;
(b) individual or collective training actions;
(c) protective measures in the worst cases;
(d) improvement of procedures, tools or design of the tasks.

4.4.4.5. Validation of corrective actions

[G 1] The effectiveness of the corrective actions is validated in order to verify that the measures of the action plan are closing the identified non-compliances. This validation or non-compliance closing can consist in a new hierarchical checking of whether the considered non-compliance is removed or still observed on the field.

4.5. Monitoring management

[G 1] This section answers the question **"Q 4: How is the monitoring to be managed?"**

[G 2] The company monitoring strategy is included in the Monitoring Plan. The different monitoring tools (return of experience, hierarchical checks, internal audits, internal incident and accident investigations, etc.) are used in line with that plan to verify the achievement of the safety requirements and safety targets, or lead to the implementation of appropriate corrective measures when non-compliances are detected. The purpose of this monitoring "Plan-Do-Check-Act" process is to ensure an effective and safe "safety management system" on a continuous basis.

[G 3] In addition to those monitoring activities, the effectiveness of the whole monitoring strategy and plan is regularly checked through specific internal audits. The objective of those audits is to measure and improve, when necessary, the quality and performance of the monitoring methods. To this end, the monitoring strategy includes an analysis of the collected monitoring data and information. The results of this analysis are provided to the top managers of the company to support them in their decision to maintain or improve the measured safety level.

5. Example 5: Example on other monitoring guidance

5.1. Context of the example

Table 38: Design of monitoring by a Railway Undertaking.

Kind of railway actor	Not applicable
Articles and/or sections in the Annex of Regulation 1078/2012 that the example most closely relates to	The example is mainly connected to the monitoring process [Article 4] and section 2 in the annex of Regulation 1078/2012
Description of the example, including among others: • its scope; • how it fits within the overall monitoring framework; • a brief summary of the content; • any limitations: *all process steps are not shown, all details of the process step are not presented; only examples are shown, etc.;* • who uses the example; • other relevant information	The example is an extract of parts of a guideline on Safety Assurance at the Company to Company level, i.e. covering interfaces, written by the UK Rail Safety and Standards Board (RSSB). Included in the guidance is one example which shows a systematic approach to the monitoring process between, in this case, a railway undertaking and an infrastructure manager. The approach is also applicable for other companies.
How could it be used by other actors?	This example of guidance could be used by infrastructure managers (IMs), railway undertakings (RUs) and entities in charge of maintenance (ECMs) when developing their Monitoring Strategy and Plan. It should be particularly useful when developing the monitoring processes for risks at the interface with other transport operators.

5.2. Introduction

[G 1] The example does not explain how to define a strategy and plan for monitoring neither how to define the indicators to be monitored.

[G 2] The example considers a fictive case of a project between a railway undertaking and an infrastructure manager. The example outlines monitoring activities that can be done systematically along the different stages of the lifecycle of a project.

[G 3] The approach is also applicable for other companies.

5.3. Safety Assurance Lifecycle

5.3.1. Introduction

[G 1] Each stage in the safety management system lifecycle (see lifecycle diagram in section § 5.4) as listed below depends on exchange of the right sort of information which is determined at stage 2:

(a) 1 risk assessment;
(b) 2 procedures and organisation (i.e. development of controls);
(c) 3 control of risks (in day to day activities);
(d) 4 checks on controls;
(e) 5 review and learnt lessons (effectively a higher level repeat of stage 1);
(f) 6 improve (effectively a higher level repeat of stage 2).

[G 2] Good safety assurance, the core of which is applied in stage 4, is dependent on:

(a) all stages being done well;
(b) the earlier stages to determine what is to be assured, and;
(c) the later stages to allow the assurance process to lead to improvement.

[G 3] Risks can be "exported" by one company to another and vice versa (imported) and the controls of these risks may be the responsibility of either or both. The following diagram shows the simple divide of possible risks and controls:

Table 39: Sharing of risks.

		Risks	
		Ours	**Theirs**
Controls	**Ours**	our risks our controls	their risks our controls
	Theirs	our risks their controls	their risks their controls

[G 4] **<u>Fictive example :</u>**

<u>Remark:</u> the following fictive example of a major project is outlined at each stage of the lifecycle below in the same coloured boxes.

<u>Example:</u>

At a terminal city station four new platforms are to be built with an overhead wire power supply.

The main actors are the infrastructure manager that owns the station and the main railway undertaking but other railway undertakings will be affected

5.3.2. Stage 1 of lifecycle: Risk Assessment

[G 1] Understanding the risks at the interfaces is a necessary start to the development of a safety management system of which interaction with another SMS is an important part.

[G 2] From a list of all the company's main risks it is useful to compile a register of the interface risks. The interface companies for each of these interface risks can then be listed.

[G 3] **Fictive example :**

The main railway undertaking and the infrastructure manager need to compile a register of all safety interface risks, including:

- Construction risks to passengers, e.g.:
  - Being struck by moving plant;
  - Slipping/tripping on uneven surface;
- Transitional emergency plans:
  - Old emergency signs sending passengers the wrong way;
  - Access routes for emergency services being blocked;
- Electrification risks that are new to the station:
  - Staff carrying ladders near electrified wires;
  - Staff washing train windscreens near electrified wires;
- Risks to infrastructure manager, railway undertaking and other railway undertakings staff:
  - Staff not knowing temporary safe walking route.

5.3.3. Stage 2 of lifecycle: Procedures and Organisation

[G 1] Companies should have procedures and organisational provisions in place to control the risks arising from the interfaces and then to obtain and exchange the information necessary for the safety assurance.

[G 2] It is necessary to analyse the register of interface risks and to agree on the risk controls with the interfacing companies.

[G 3] For that, it is necessary to determine how to obtain the necessary information, e.g. from the following information sources, but this list is not exhaustive:

(a) audits (joint audits, audit findings from other's audit or audit of other);
(b) setting Safety Performance Indicators (SPIs) and monitoring via Safety Performance Reports (include fault reporting systems);
(c) inspections (as for audits);
(d) accident investigation outputs/recommendations;
(e) peer review;
(f) consider future risks to ensure good safety assurance is maintained (and later report on these):
    (1) planned activities with new risks e.g. projects;
    (2) proposed changes that bring different risks.

[G 4] Determine then how to exchange information.

[G 5] Good safety assurance would benefit from a formal agreement[(17)] with companies that share risks at the interfaces to give a formal and detailed agreement.

[G 6] **Fictive example :**

> The infrastructure manager and railway undertaking review the register of risks and agree on individual and joint controls, e.g.:
>
> - Weekly briefing of key staff;
>
> They also agree on how to check on the various controls and what should be deemed as acceptable, e.g.:
>
> - Joint audits/inspections to include questions on whether staff have had effective briefings, having agreed that 90% must be completed and 90% of these must be judged to be effective.

5.3.4. Stage 3 of lifecycle: Control of Joint Risks

> [G 1] Having assessed the risks and determined how they will be controlled this stage of applying the controls is the day-to-day business of the company

[G 2] **Fictive example :**

> The railway undertaking and infrastructure manager proceed with the project, implement the controls and undertake the agreed checks such as joint audits/inspections.

(17) *Note that the regulation requires contractual arrangements in Article 4(1)*

5.3.5. Stage 4 of lifecycle: Joint Check on Effectiveness of Controls

[G 1] This is the core of safety assurance, i.e. the combination of activities through which managers learn that agreed controls are being properly applied and that they are effective in controlling the assessed risks.

[G 2] This is the conscious checking that controls are being properly applied and that they are effective in controlling the assessed risks. Sources of information used to check the effectiveness are listed above in point [G 3] of section § 5.3.3 and in some cases examples are given below.

[G 3] **Audits:**

There are many options on the types of audits (for example joint audits) that could be used to check on the effectiveness of the control of interface risks. They could be any of the following, with the findings being shared with the interface companies:

(a) Company A on interface Company B;
(b) Company A on itself;
(c) Jointly run by Company A and B;
(d) Third party on Company A and/or B, commissioned by A and/or B;
(e) etc.

[G 4] **Reports on Safety Performance Indicators (SPIs):** these could be "jointly set indicators", e.g. during a common project.

[G 5] **Peer Review:** the industry may wish to consider something similar to the process used by the nuclear industry: World Association of Nuclear Operators (WANO).

[G 6] **Fictive example :**

All information should be collected and filtered to be suitable for the level of review, e.g.:

- the number of inspections undertaken, say 80%, gives limited information;
- a summary of the effectiveness of the application of the controls will probably be more useful, e.g.:
  - a professional judgment on effectiveness of briefings;
  - key problems identified and addressed;
  - key problems still to be resolved.

5.3.6. Stage 5 of lifecycle: Review and Lessons Learnt

[G 1] This stage is crucial to the assurance of safety. Risk based and intelligent review of the relevant information by the right people should lead to the important lessons being learned

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] The safety assurance information gathered from the various sources should be reviewed by the appropriate people at the right levels and a joint review will be appropriate in some cases. This should include high level review of filtered information to allow well informed decision making.

[G 3] The review process should include consideration of consistency of findings from different sources, e.g. an audit may give bad impression but the monitoring of the safety performance the opposite.

[G 4] The learning of lessons will lead to changes and these should be integrated into the Safety Management System and its supporting procedures.

[G 5] A good review will do more than confirming that boxes have been ticked (audits have taken place) but will consider trends, dwell more on the bigger outstanding risks, consider the impact of change and will compare intelligence from different sources to fully understand any variance in the safety picture given from the different sources.

[G 6] **Fictive example :**

Jointly review the effectiveness of the controls, e.g.:

- at a monthly joint meeting with a standing agenda;
- well informed review of relevant data;
- resolve problems;
- change controls and/or monitoring, e.g.:
  - ensure information on the following weeks changes and risks are supplied to those doing the briefings.

5.3.7. Stage 6 of lifecycle: Improve

[G 1] This could be considered to be beyond the remit of safety assurance but if it is not done. It does undermine the whole SMS lifecycle and improvement process. It is important that agreed improvements are integrated into the SMS and its application. This will include changing the SMS and related policies and procedures, necessary training and briefing, changes to indicators and then monitoring impact and ultimately review of effectiveness

5.4. Lifecycle of safety assurance at the Company–to–Company level

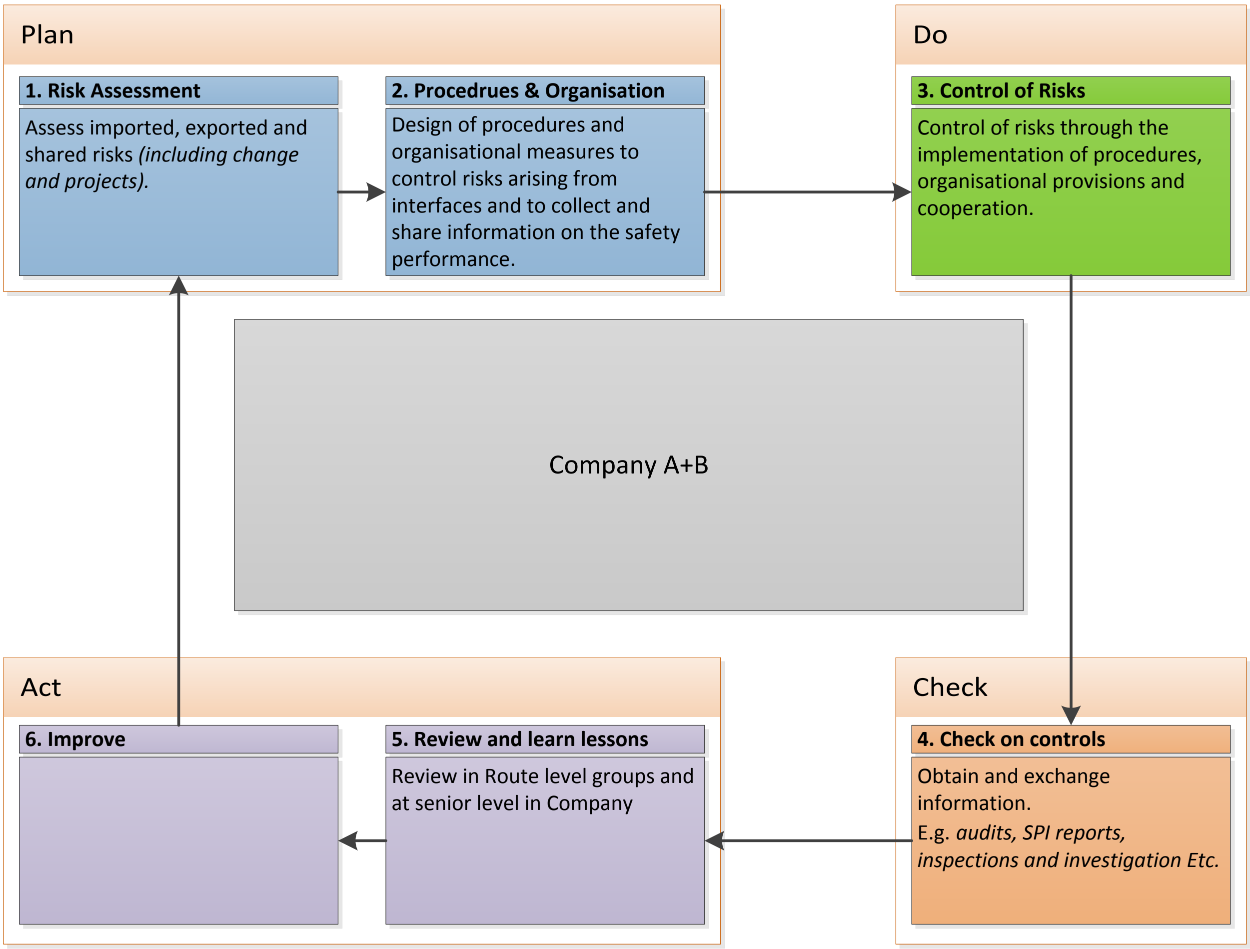


Figure 29: Lifecycle of safety assurance at the Company–to–Company level.

6. Example 6: Design of monitoring by an entity in charge of maintenance (ECM)

6.1. About the example

Table 40: Design of monitoring by an entity in charge of maintenance (ECM).

Kind of railway actor	Entity in charge of maintenance
Articles and/or sections in the Annex of Regulation 1078/2012 that the example most closely relates to	The example is mainly connected section 2 in the annex of Regulation 1078/2012. It focuses on the definition of the indicators.
Description of the example, including among others: • its scope; • how it fits within the overall monitoring framework; • a brief summary of the content; • any limitations: *all process steps are not shown, all details of the process step are not presented; only examples are shown, etc.;* • who uses the example; • other relevant information	This example shows an approach how to design the monitoring for ECM. It also shows examples on indicators for an ECM. Note that the list of indicators is not exhaustive.
How could it be used by other actors?	It shall be seen as an example on one way to define indicators for an ECM. Other ways are also possible. It is meant to be a help for ECMs to settle and/or formalise their own monitoring activities. A brief approach on the definition of safety targets it is presented.

6.2. Definition of a strategy for monitoring

[G 1] The purpose of the monitoring activity is to enable the effective management of safety in the railway system during its operation and maintenance activities.

[G 2] The Directive 2004/49/EC defines some minimum items to be surveyed to ensure that the safety level does not degrade. In the present example, an entity in charge of maintenance (ECM) for freight wagons has done a brainstorming exercise and tried to translate those minimum items into measurable parameters on a freight wagon.

[G 3] As a first input, only the technical aspects are taken into account. The results of the brainstorming are reported in the matrix below.

[G 4] Using its return of experience, the ECM tried to define an order of priority for every event. That is the first step of the prioritisation.

[G 5] Based on that prioritisation and brainstorming results, the ECM identified the events to be monitored for each wagon and some other events that should be taken as a statistical survey:

(a) W: No wagon should present this defect

If an event, classified as W, occurs, investigations should be carried out and a report written to record the decisions taken, when applicable.

(b) S: Statistical surveillance of the wagon fleet

An acceptable level is defined by the ECM and an alarm is raised when it is exceeded.

6.3. Matrix of the items to be monitored by an ECM

[G 1] The matrix below contains the items to be monitored by an ECM.

[G 2] It should be completed with the specificity of the wagon types the ECM is dealing with, as well as with the organisational and operational aspects linked to its size and scope of activity.

Table 41: Matrix of the items to be monitored by an ECM.

RISC MANAGEMENT IN RAILWAY SYSTEM LINKED TO MAINTENANCE ACTIVITY OF FREIGHT WAGONS : Safety targets for sub system "freight wagon"

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*C*
	Wagon feared events (Safety target for ECM)					**Feared events for railway sector (Safety directive)**							
	Function	**Event or risk of event [18]**	**Examples**	**Safety target**		**Fire Explosion of wagon**	**Derailment Overturn**	**People's injury**	**Collision**	**Infra-structure's fire**	**Environ-ment's Pollution**	**Accident at level crossing**	**Event or risk of event [19]**
Inter-operability with RUs	***Information / Lettering for wagon incorporation in trains***	Wrong information on braking characteristics	Brake Weight, Load sheet	W					X	X			Wrong information on braking characteristics
	Information / lettering for loading	Wrong or missing information for loading	Container transport loading Loading of coils Dangerous goods - Information of transported material Gas transport wagon - Phases identification interverted	W		X	X	X	X	X	X	X	Wrong or missing information for loading

(18) *Event or risk of event that could endanger the actual level of safety*

(19) *Event or risk of event that could endanger the actual level of safety*

Table 41: Matrix of the items to be monitored by an ECM.

RISC MANAGEMENT IN RAILWAY SYSTEM LINKED TO MAINTENANCE ACTIVITY OF FREIGHT WAGONS : Safety targets for sub system "freight wagon"

A	B	C	D	E	F	G	H	I	J	K	L	M	C
	Wagon feared events (Safety target for ECM)					**Feared events for railway sector (Safety directive)**							
	Function	**Event or risk of event [18]**	**Examples**	**Safety target**		**Fire Explosion of wagon**	**Derailment Overturn**	**People's injury**	**Collision**	**Infra-structure's fire**	**Environ-ment's Pollution**	**Accident at level crossing**	**Event or risk of event [19]**
	Information / lettering for operations	Wrong information on load sheet	Regime S/ SS, Loads	W			X						Wrong information on load sheet
		Wrong gauge Information		W				X	X				Wrong gauge Information
Wagon Inter-operability	***Brake***	Braking system blocked		W		X	X			X			Braking system blocked
		Incompatible reliability rate of braking system		S					X				Incompatible reliability rate of braking system
		Braking system inter-operability	Comply with referential	S					X	X			Braking system interoperability
	Continuity / Integrity of the train	Split of permanent coupling	Double wagons, doubled elements	W			X		X				Split of permanent coupling
		Loss of pieces	Boards (inscriptions,…)	W			X	X	X				Loss of pieces
			broken step, broken handling rail	W			X	X	X				

Table 41: Matrix of the items to be monitored by an ECM.

RISC MANAGEMENT IN RAILWAY SYSTEM LINKED TO MAINTENANCE ACTIVITY OF FREIGHT WAGONS : Safety targets for sub system "freight wagon"

A	B	C	D	E	F G	H	I	J	K	L	M	C
	Wagon feared events (Safety target for ECM)				**Feared events for railway sector (Safety directive)**							
	Function	**Event or risk of event** [18]	**Examples**	**Safety target**	**Fire Explosion of wagon**	**Derailment Overturn**	**People's injury**	**Collision**	**Infra-structure's fire**	**Environ-ment's Pollution**	**Accident at level crossing**	**Event or risk of event** [19]
		Under frame broken		W		X		X				Under frame broken
		Wheelset broken		W		X		X				Wheelset broken
		Bogie broken	Defective soldering work	W		X		X				Bogie broken
		Loss of load	Leaking tank, bin, …	W		X	X	X		X	X	Loss of load
			Unexpected opening of doors, hatch, other sealing system, …	W		X	X	X		X	X	
	Stability	inefficient suspension	Broken spring, defective absorbing system	S		X	X	X				inefficient suspension
		Wheelset geometry out of tolerances	Wheel profile and or wheel spacing	W		X						Wheelset geometry out of tolerances

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table 41: Matrix of the items to be monitored by an ECM.

RISC MANAGEMENT IN RAILWAY SYSTEM LINKED TO MAINTENANCE ACTIVITY OF FREIGHT WAGONS : Safety targets for sub system "freight wagon"													
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*C*
	Wagon feared events (Safety target for ECM)					**Feared events for railway sector (Safety directive)**							
	Function	**Event or risk of event [18]**	**Examples**	**Safety target**		**Fire Explosion of wagon**	**Derailment Overturn**	**People's injury**	**Collision**	**Infra-structure's fire**	**Environ-ment's Pollution**	**Accident at level crossing**	**Event or risk of event [19]**
		Incompatible rotation torque between bogie and under frame	Worn centre casting, No gap on the side friction block	W			X						Incompatible rotation torque between bogie and under frame
		Incompatible compression force	Damaged buffer head	W			X						Incompatible compression force
Inter-operability with infra-structure	***Gauge***	Failure of the load fixing system causing an interference with gauge	Damaged bar chock, Door opening, …	W			X	X	X				Failure of the load fixing system causing an interference with gauge
		Incompatible wheelsets	Wheelset diameter out of tolerances	W			X	X	X				Incompatible wheelsets
		wagon parts deformed or worn	Worn or deformed stanchion, friction block failure, applied parts failure	W			X	X	X				wagon parts deformed or worn

Table 41: Matrix of the items to be monitored by an ECM.

RISC MANAGEMENT IN RAILWAY SYSTEM LINKED TO MAINTENANCE ACTIVITY OF FREIGHT WAGONS : Safety targets for sub system "freight wagon"

A	B	C	D	E	F	G	H	I	J	K	L	M	C
	Wagon feared events (Safety target for ECM)					**Feared events for railway sector (Safety directive)**							
	Function	**Event or risk of event (18)**	**Examples**	**Safety target**		**Fire Explosion of wagon**	**Derailment Overturn**	**People's injury**	**Collision**	**Infra-structure's fire**	**Environ-ment's Pollution**	**Accident at level crossing**	**Event or risk of event (19)**
		Loose mobile parts	Non expected opening of doors, stanchion, …	W			X	X	X				Loose mobile parts
	Signalling	De shunting	Bad shunting wheel, loss of product (salt, …), non-authorised K brake blocks	W					X			X	De shunting
	Signalling	Noises on radio frequency	Non filtered electro generator	W					X			X	Noises on radio frequency
	Tracks infrastructure	Incompatible wheelset geometry	Wheelsets geometry non compatible with switch points, track switch	W			X						Incompatible wheelset geometry
Health and safety		Uncontrolled process for recycling polluting wagon components	While destructing a wagon, recycling process of asbestos, ceramics, boards with creosote oil, …	W				X			X		Uncontrolled process for recycling polluting wagon components

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Table 41: Matrix of the items to be monitored by an ECM.

A	B	C	D	E	F	G	H	I	J	K	L	M	C
	RISC MANAGEMENT IN RAILWAY SYSTEM LINKED TO MAINTENANCE ACTIVITY OF FREIGHT WAGONS : Safety targets for sub system "freight wagon"												
	Wagon feared events (Safety target for ECM)					**Feared events for railway sector (Safety directive)**							
	Function	**Event or risk of event [18]**	**Examples**	**Safety target**		**Fire Explosion of wagon**	**Derailment Overturn**	**People's injury**	**Collision**	**Infra-structure's fire**	**Environ-ment's Pollution**	**Accident at level crossing**	**Event or risk of event [19]**
		Sound pollution	Wheel tread damaged through braking system	S							X		Sound pollution
A	B	C	D	E	F	G	H	I	J	K	L	M	C

"interoperability": ability of a railway system to enable safe running and without train split while to achieve the required performances on the relevant railway lines. This ability depends on all legislative, technical and operational conditions that must be fulfilled in order to comply with the essential requirements.

W : Goal : 0 wagon reported with this defect

S : Statistical goal on the wagon fleet

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

7. Example 7: Monitoring by a manufacturer

7.1. About the example

Table 42: Monitoring by a manufacturer.

Kind of railway actor	Supplier/Manufacturer
Articles and/or sections in the Annex of Regulation 1078/2012 that the example most closely relates to	The example is mainly connected to Article 4(2) of Regulation 1078/2012. It focuses on the necessary sharing of information through the interfaces to enable other parties to take any necessary corrective actions.
Description of the example, including among others: • its scope; • how it fits within the overall monitoring framework; • a brief summary of the content; • any limitations: *all process steps are not shown, all details of the process step are not presented; only examples are shown, etc.;* • who uses the example; • other relevant information	The example shows a process how to deal with Potential Safety Deficiencies (PSD) of technical equipment, which occur at the interface of a supplier/manufacturer and a railway undertaking or an infrastructure manager. Usually such a process is embedded in the safety management system of the railway undertaking or infrastructure manager and the complaint management process of suppliers. The particular example methods are given to illustrate the process to apply to any fault, which is either of statistical or systematic nature. Not all details of the particular methods are given here. The approach is standardised in a German standard DIN V VDE V 0831-100 for railway signalling applications and has been practiced mainly by German suppliers for more than 5 years. However it is also used in international business of these suppliers. It should be noted that the standardisation has benefited from the CSM regulation on risk assessment, as several concepts and principles of the regulation have been applied.
How could it be used by other actors?	The process and the particular methods can be directly applied based on the complete description in DIN V VDE V 0831-100. The process is compatible with the Regulation on the CSM for monitoring.

7.2. Introduction

[G 1] The supervision of technical equipment or products by their manufacturers or the monitoring activities by a railway undertaking or an infrastructure manager can reveal the occurrence of more frequent safety-relevant events than expected or possibly undetected systematic errors of these technical equipment or products. In both cases, a Potential Safety Deficiency (PSD) is identified. This means that one of the parties (i.e. a railway undertaking, an infrastructure manager or a manufacturer) concludes that the technical equipment/product is not any more compliant with the initial assumptions and safety assessments (safety situation has changed) so that a reporting of the problem to all involved or affected parties is essential.

[G 2] This situation can be illustrated by the two used cases below.

[G 3] Case 1 - related to a frequency of failure higher than expected in the risk assessments:

(a) an operator suspects that a new product fails in-service more often than a proven-in-use reference system (e.g. for a door control system the operator receives a large number of incident reports). He contacts the supplier of the new system because he suspects a Potential Safety Deficiency (PSD);

(b) two safety requirements are specified in the system requirement specifications of the customer for an automatic train protection (ATP) system:

(1) a hazard rate (HR) for the direct safety function (the ATP does not brake the train in case of a signal passed at danger - SPAD), and;
(2) a failure rate (FR) (the ATP system does not work, so that the operational safety depends directly on the driver in the fall back mode).

From his product supervision (feedback data from multiple customers) the supplier suspects that a predictive quantitative requirement (HR or FR) may not be met in practice.

[G 4] Case 2 - related to systematic failures not detected and not corrected during design:

(a) for example, the staff from an operator reports that a signal, which should have been red, showed a green aspect for some seconds. The operator contacts the system integrator for clarification, who finds a systematic cause, which has so far not been observed before;

(b) during the acceptance tests of a new product a supplier detects a software fault in a re-used component, which appears only under specific circumstances and has not been reported from the field so far. The component is used in several in-service systems by several customers.

7.3. Definition of a strategy for monitoring and of indicators

[G 1] The objective of a Potential Safety Deficiency (PSD) assessment is to assess a potentially changed safety situation of a technical equipment/product and, if required, to take additional measures for ensuring that the system affected by the PSD offers at least the same level of safety as a reference system (which may, for example, be the approved system without a PSD). Thus the principle used as a basis is ALASA (At Least As Safe As) or GAMAB/GAME compared to a reference system.

[G 2] For both used cases explained above the procedure is similar: the number of failures reported serves as an indicator, and if a particular threshold is exceeded then a non-compliance is detected. For systematic failures the threshold is usually 0, while for other failures the threshold is determined by statistical reasoning.

[G 3] The German standard DIN V VDE V 0831-100 explains in detail the individual process steps that should be taken in the flow diagram in Figure 10. The left side of Figure 10 gives the overall process; the right side one represents a particular evaluation process. This example describes only the basic steps; details must be regulated in the operator's or supplier's safety or quality management system (in particular the complaint management process). Depending on the selected procedure, the process steps may include sub-steps which, for reasons of brevity, are not dealt with in detail here.

7.4. Description of the process

7.4.1. Similarity with the Regulation on CSM for monitoring

[G 1] The process shown in Figure 10 corresponds to the Monitoring Process defined in the appendix of the Regulation on the CSM for monitoring, as both are implementations of the "Plan-Do-Check-Act" principle.

[G 2] The monitoring strategy and indicators representing the plan have been defined above and the following steps are similar to the process steps, mainly "Collection and analysis of information". Steps 3 to 7 correspond to the "Analysis and evaluation of non-compliances".

7.4.2. 1st step – Start-up of the PSD assessment process

[G 1] At the start-up of the process (which corresponds to the "Identification of non-compliances" step in the regulation) and possibly also during each process step the initiator (operator or supplier) must check whether the Potential Safety Deficiency (PSD) meets the following requirements:

(a) the PSD can occur in a system in operation;
(b) the PSD affects a safety-related function (SIL >0);
(c) the PSD has a risk-increasing effect (compared to the explicit safety requirement).

[G 2] For case 1 (related to an increased frequency of failure) condition 3 is usually evaluated by a statistical procedure. Let us also assume that the considered electronic component S is approved in-service, and it was designed to satisfy a quantitative requirement FR for a particular failure.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

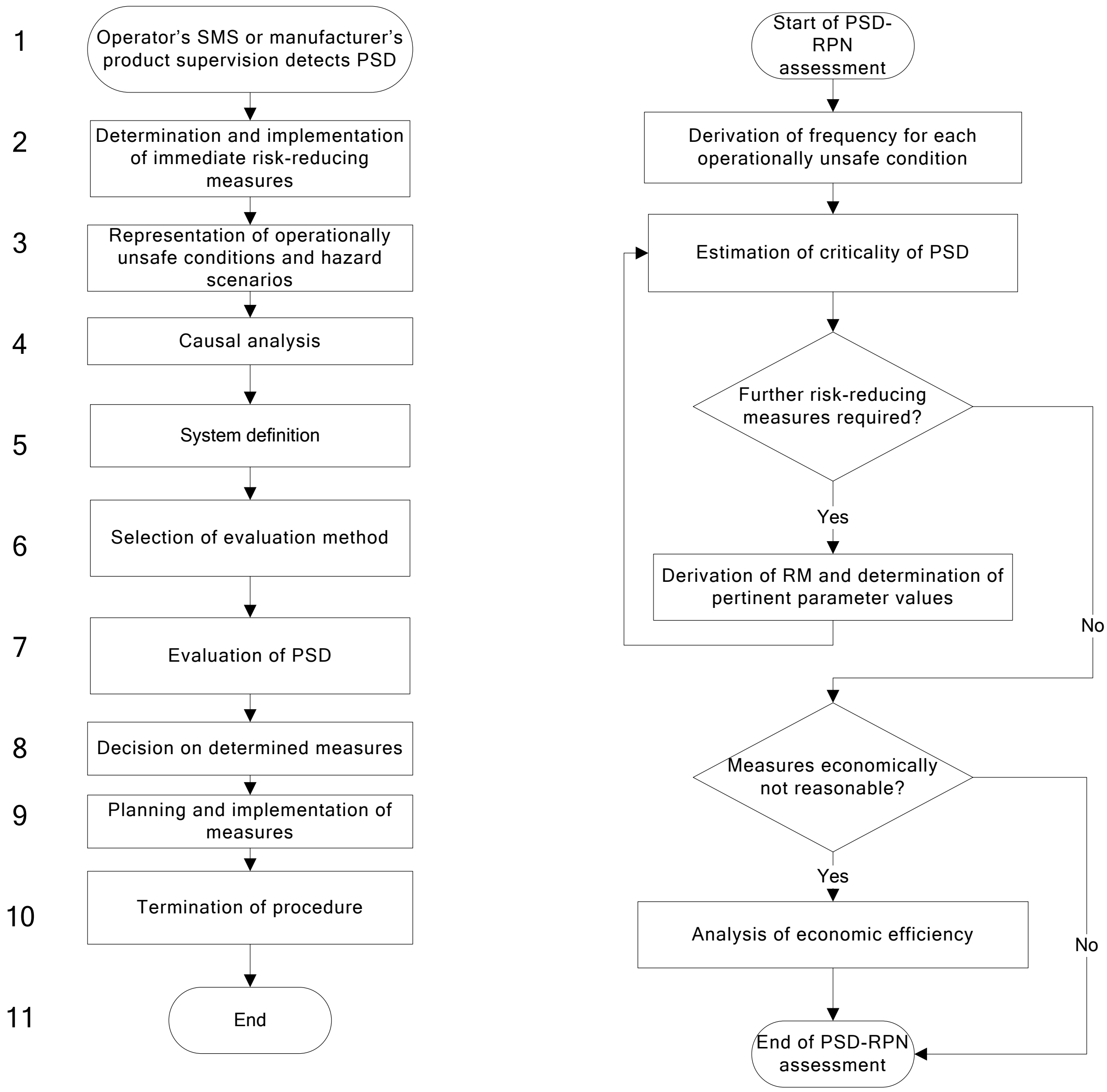


Figure 30: Process flow diagram – General and detailed.

[G 3] S has been in service under similar conditions for t_S hours and x_S occurrences of the failure condition have been reported so far. From IEC 60605-4 standard it is known that the hypothesis that S fulfils the requirement FR should be rejected if

$$\frac{\chi^2_{\alpha,2x_S}}{2t_S} > FR \qquad \textbf{Equation [1]}$$

[G 4] This condition means that FR (*i.e. the failure rate representing that the technical equipment/product is defective so that that the operational safety depends directly on human operators in a fall back mode*) is not covered by the corresponding confidence band of the data. To illustrate this let us give an example with FR = 10^{-5} h^{-1} and an

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

operation experience of 100 components over 1 year. During that period, 13 failures were observed. The statistical estimate is about 3 x 10^{-5} h^{-1}. However for α = 0,05 error probability the deviation is not significant as the calculated test statistic is only about 9 x 10^{-6} h^{-1}. So the evaluation has shown that the deviation is within expected statistical limits and the failure data should be monitored further but no corrective action is necessary at this time and the process is not started.

[G 5] If one of the conditions does not apply to an occurred Potential Safety Deficiency (PSD), the process should not be started. Alternatively, if it is discovered at a later date that a condition does not apply, the process should be aborted and terminated with documented evidence.

7.4.3. Immediate measures

[G 1] Depending on the severity or extent of the event, immediate corrective measures must be taken by the operator within the framework of the hazard avoidance. During the further process these immediate measures can be cancelled again after a detailed analysis of the Potential Safety Deficiency (PSD) and/or replaced by other medium or long-term measures.

7.4.4. Representing operationally unsafe conditions and hazard scenarios

[G 1] An operationally unsafe condition caused by a Potential Safety Deficiency (PSD) exists if other planned barrier which might prevent an unwanted event do not exist in the overall system: see Figure 31.

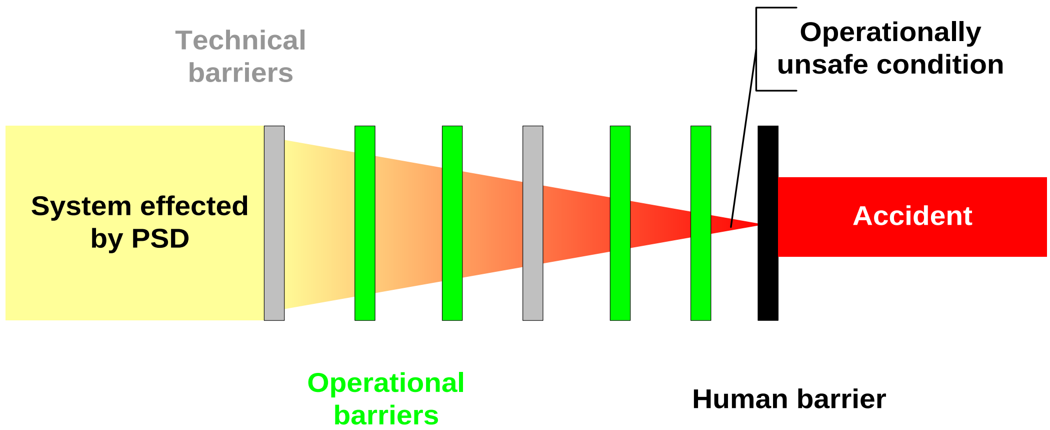


Figure 31: Basic Model for representing Operationally Unsafe Conditions and Hazard Scenarios.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] A hazard scenario is a path leading from the fault via the barriers towards the operationally unsafe condition and the accident. All credible hazard scenarios caused by the Potential Safety Deficiency (PSD) must be described concisely. The hazard scenarios must be aligned with the hazard log or integrated into this log. This process step is performed by the operator, often in cooperation with the supplier.

7.4.5. Causal analysis

[G 1] The possible causes of the Potential Safety Deficiency (PSD) must be analysed on the basis of the hazard(s) found in the above step. The causes may be located in different sub-systems of the railway system or also in ambient systems. For technical systems this is mainly performed by the supplier, but there may be causes related to operations as well.

7.4.6. System definition

[G 1] If the causing system is known, a definition of that system must be created or referenced according to the requirements given in the Regulation on the CSM for risk assessment. For technical systems this is usually performed by the supplier in cooperation with the operator.

7.4.7. Selection of evaluation methods

[G 1] In this step it is decided which kind of risk evaluation method is chosen, e.g. qualitative, semi-quantitative or quantitative, depending on the type of problem and the data and information available. This has to be agreed by the supplier and the operator.

7.4.8. Evaluation of a Potential Safety Deficiency (PSD)

[G 1] The evaluation depends on the type of the problem and of the evaluation methods. The particular method proposed in the standard is mainly focusing on case 2 problems but can be used for case 1 as well.

[G 2] The right side of Figure 10 gives a particular implementation of step 7 of the general process, which is the risk-based evaluation of the Potential Safety Deficiency (PSD). It consists of an iterative assessment of the criticality of the unsafe situation by a semi-quantitative method (called PSD-RPN) and the evaluation of risk-reducing measures. The risk evaluation is based on a particular risk matrix (see Table 43), which puts a semi-quantitative risk estimation in relation to the safety requirements (expressed as a Safety Integrity Level - SIL) in order to determine whether further risk reduction measures are necessary and the tolerable time for fault removal. Further details can be found in the references.

[G 3] Finally, if the measures are economically not reasonable, but the resulting residual risk is broadly acceptable according to the Regulation on the CSM for risk assessment, then it can also be decided not to implement particular measures. Broadly acceptable risk is interpreted as in the guidelines of the European Railway Agency on the application of the Regulation on the CSM for risk assessment or as ALARP, which means that the additional risk is below 1% of the original safety requirement.

[G 4] As an example, let us assume that a Potential Safety Deficiency (PSD) in a SIL 1 ATP system is discovered. The initial analysis of the causes and the hazard scenarios lead to a semi-quantitative risk estimate of 11, which would mean that the fault must be removed within 1 month in the complete fleet. As this seems too demanding another risk reducing measure is proposed which reduces the semi-quantitative risk estimate to 9, which extends the tolerable fault removal time to 12 months.

Table 43: Risk matrix for the determination of the fault removal time.

<table>
<tr><th>H-ΔRM</th><th>SIL1 Function</th><th>SIL2 Function</th><th>SIL3 Function</th><th>SIL4 Function</th></tr>
<tr><td>0</td><td rowspan="8">60 months</td><td rowspan="6">60 months</td><td rowspan="4">60 months</td><td rowspan="2">60 months</td></tr>
<tr><td>1</td></tr>
<tr><td>2</td><td>36 months</td></tr>
<tr><td>3</td><td>12 months</td></tr>
<tr><td>4</td><td>36 months</td><td>4 months</td></tr>
<tr><td>5</td><td>12 months</td><td>1 month</td></tr>
<tr><td>6</td><td>36 months</td><td>4 months</td><td rowspan="6"></td></tr>
<tr><td>7</td><td>12 months</td><td>1 month</td></tr>
<tr><td>8</td><td>36 months</td><td>4 months</td><td rowspan="4">Further risk reducing measures are required</td></tr>
<tr><td>9</td><td>12 months</td><td>1 month</td></tr>
<tr><td>10</td><td>4 months</td><td rowspan="2"></td></tr>
<tr><td>11</td><td>1 month</td></tr>
<tr><td>>11</td><td colspan="4"></td></tr>
</table>

7.4.9. Decision on determined measures

[G 1] If in one of the above process steps additional measures were selected, the decision on the application must be taken on the management level of the operator in this step. This step corresponds to “Definition of an Action Plan”. Here iterations of the preceding process steps are possible.

7.4.10. Planning and implementation of the measures

[G 1] The measures decided in the preceding process steps must be planned and implemented in this step. This corresponds to the step “Implementation of the Action Plan”.

7.4.11. Termination of the procedure

[G 1] After the selected additional measures have been implemented, the risk reducing measures no longer required can be cancelled. This includes in particular the removal of the fault which caused the problem. This step corresponds to “Evaluation of the effectiveness of the action plan measures”.

7.5. Summary

[G 1] The example described a process which is based on a German standard, see DIN (2009). Details on a particular implementation and examples for its application can be found in Braband (2011). The process and the particular semi-quantitative risk evaluation method described have been successfully practiced, mainly by the supply industry but also operators, not only in Germany, but worldwide.

7.6. References

[G 1] More information about this technique for Potential Safety Deficiency assessment can be found in the following references that were used as input for writing this example:

(a) Braband (2011) - Risk-based Decision Support in relation to Potential Safety Deficiencies, in Proc. World Congress in Railway Research (WCRR2011), Lille 2011;

(b) DIN (2009) Risikoorientierte Beurteilung von potenziellen Sicherheitsmängeln und risikoreduzierenden Maßnahmen. DIN V VDE V 0831-100;

(c) ERA (2009): Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of the Railway Safety Directive, ERA/GUI/01-2008/SAF;

(d) IEC 60605-4 Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals

8. Example 8: Monitoring by a manufacturer

8.1. About the example

Table 44: Monitoring by a manufacturer.

Kind of railway actor	Supplier/Manufacturer
Articles and/or sections in the Annex of Regulation 1078/2012 that the example most closely relates to	The example is mainly connected to Article 4(2) of Regulation 1078/2012. It focuses on the necessary sharing of information through the interfaces to enable other parties to take any necessary corrective actions.
Description of the example, including among others: • its scope; • how it fits within the overall monitoring framework; • a brief summary of the content; • any limitations: *all process steps are not shown, all details of the process step are not presented; only examples are shown, etc.;* • who uses the example; • other relevant information	This example illustrates how the feedback from in-service performance of a piece of equipment, in this case a defective rolling stock system, can provide proactive management of potential safety issues and help to manage future potential safety incidents.
How could it be used by other actors?	It shall be seen as an example on one way to exchange safety relevant information from the field.

8.2. Introduction

[G 1] The railway undertakings, infrastructure managers and entities in charge of maintenance are often not in possession of all of the technical design file and manufacturing details as to how the product was designed and built. Therefore from time to time the original technical design file data may need to be consulted to ascertain if a deviation observed during monitoring activities by those actors is significant or not.

[G 2] This assessment requires therefore an exchange of information between the railway undertakings, infrastructure managers and entities in charge of maintenance and their suppliers.

European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

8.3. Example

[G 1] A routine planned maintenance check on the door system of a commuter train reveals a crack starting to grow in the door header bracket. This bracket is part of the door fixing mechanism to the body shell of the train. The operator is notified about the occurrence of the problem and in turn so is the supplier.

[G 2] Initially, the cause of the starting crack is identified as an extreme environmental and operational condition outside the original design specifications.

[G 3] New calculations and modelling demonstrate that crack is not overall structural integrity of the door fixing provided that it is below a threshold (e.g. 5 mm). Several checks across the fleet and over time show that the crack is limited to a few installations and the crack has not developed over time. A new monitoring check is therefore introduced in the maintenance instruction to check periodically for the presence and length of any cracks.

[G 4] A new design is proposed by the supplier to eliminate this failure mode. The environmental and operating conditions experienced in this application are logged by the manufacturer for future use. The information is also communicated to other potentially affected parties.

8.4. Discussion

[G 1] According to Article 4(3) of Directive 2004/49/EC infrastructure managers and railway undertakings are responsible for the safe operation of the railway system and the control of risks associated with it.

[G 2] According to Article 4(4) of Directive 2004/49/EC, each manufacturer (among others) is responsible to ensure that rolling stock, installations, accessories and equipment and services supplied by them comply with the requirements and the conditions for use specified, so that they can be safely put into operation by the railway undertakings and/or infrastructure managers.

[G 3] If any of those actors becomes aware of a safety issue relevant for another actor, actions should be taken or information should be sent as the responsible thing to do from an overall safety point of view. This is also required by Article 4(2) of Regulation 1078/2012 on the CSM for monitoring.

[G 4] However in the subsequent investigation and resolution of the issue several factors will come into play. Firstly, the fact that the primary safety responsibility is within the safety case holders (railway undertakings and infrastructure managers) and then the entity in charge of maintenance (ECM). They may choose to address the issue in whatever manner they feel is appropriate under their responsibility.

[G 5] Likewise for the supplier/OEM (Original Equipment Manufacturer) which may have provided the piece of equipment that is now operating for many years out of warranty and after many maintenance and overhaul interventions, and possibly modifications. The original design and build assumptions may have therefore evolved over time in service operation.

[G 6] The decision to involve the supplier/OEM would hence typically be based on a contractual arrangement (in case of a design fault defined under warranty conditions) or a commercial basis between two parties where each agrees the share of the costs associated in the investigation, design, resolution and retrofit costs of any proposed changes.