UNIFE

Comments on SAMRAIL Report

Work Packages 2.1 to 2.8

1 Aim and structure of the report

The projects SAMNET and SAMRAIL, set up and founded by the European Union, have the aim to create basic information which is later on used by the European Railway Agency to help develop mandatory European rules. Although the industry will delegate representatives in the working groups of the European Railway Agency, results and proposals from SAMNET and SAMRAIL could lead to future difficulties. Therefore the industry (on European level represented by UNIFE) wishes to point out potential difficult issues in the SAMRAIL reports. The aim is to address these issues in the frame of the SAMNET forum running until 31.12.2005.

The VDB (German railway industry association) has elaborated the following comments for UNIFE. As a first step the comments on the different work packages of SAMRAIL are given. These comments were discussed and agreed with the VDB working groups "Signalling Rules" and "Rolling Stock" and then as a second step merged into a single report. As a third step the merged report was then agreed with the two VDB working groups.

The VDB comments are limited to those items affecting the industry directly or indirectly. No comments are given regarding those items related to other bodies such as. railway undertakings, infrastructure managers. There are also no comments made on proposals which are considered to be fully in line with the European Safety Directive.

The content of this report is endorsed by UNIFE after its review by the innovation and harmonisation committee and the UNIFE strategy group.

2 Summary

- The goal *"Develop an approach that will guarantee the safety of the railways of the European Union, taking into account the social and economic needs of the community and the diversities of the legal and regulatory systems and considering cost-effective technical and scientific innovations"* (see project brochure, version 01.10.2002, page 5) has not been reached and could be pursued through SAMNET. The SAMRAIL reports only contribute to this goal but are still far away from delivering a consistent and practicable solution to this problem.

- The reports do not represent the state of the art in all parts. The definitions are not fully consistent with those used in the new Safety Directive and the European standards (EN). The reports are presenting the viewpoint of different Member States. But they do not provide an overall European solution.

- The reports are only based on a part of all gathered experiences. There can be more and other good solutions. So the content of these reports can not be directly used as a basis for rules and other regulations to be elaborated by the European Railway Agency (ERA). In many cases the SAMRAIL results need to be reviewed, changed and adapted.

- Another problem is that generally only the signalling sector is treated in depth but the whole railway system needs to be considered. The proposals should also be valid for rolling stock, energy and civil construction. It is important to create a solution valid for all parts of the railway system.

  Very often the SAMRAIL reports take EN 50129 as basis for a proposal for the whole railway system. However, EN 50128 and EN 50129 only cover electrical, electronic and programmable systems. For all other technology (e.g. civil structures, mechanics, pneumatics, power supply) the standards do not provide sufficient guidance. Unfortunately, SAMRAIL does not answer the question how these areas should be managed with regard to risk assessment and how to quantify the hazards in case of technical failures.

  So far SIL only have been defined for electric, electronic and programmable systems. For all other technology the safety integrity concept has not been detailed and thus it is sometimes difficult or sometimes inappropriate to apply. Generally, it should be discussed whether it is reasonable at all to apply the safety integrity concept to all parts of the railway system.

  This leads to an unbalanced situation. Safety targets and safety methods should be valid for the whole railway system and then be apportioned to specific subsystems. But does it

make sense to apportion these targets and apply a common methodology to subsystems when in a wide range of the railway systems no standards exist to transfer these targets into practical technical solutions? Today often quantitative risk and hazard analyses are carried out for signalling issues. But this is seldom done in the area of rolling stock and electrical installations. Regarding civil constructions (and mechanical system in general) this is totally unusual.

3 Specific Main Comments

- The "application condition" and the "risk analysis and system requirement" must be elaborated by the railway undertakings (RU) and infrastructure managers (IM). Only these bodies can define the later application conditions of the new system and carry out a well-founded risk analysis to define the system requirements in the specific case.

  It is not clearly shown that the risk analysis has to be performed by the RU or IM on a generic level for a well defined system, sub system or component (asset). The result of this risk analysis has to be compared with the common safety target (CST) defined by the ERA. One result of the generic risk analysis are tolerable hazard rates (THR) for the asset on generic level.

- In the reports it is not clearly mentioned that the hazards not only result from technical problems. The human factor (operator, driver etc.) plays a very important role. It can be (especially in degraded modes) that the resulting safety in some cases is determined by the human factor and not so much by failures on the technical side. With regard to the influence of the human factor on the resulting safety it should be discussed what the influence of the availability of the technical part of the railway system on the resulting safety is.
  The contents are widely technicallly orientated. Human factors and organisational problems are not always respected on an acceptable level.

  Automation means to shift tasks from the human operator to technical systems. It should be mentioned that risk analyses could help select the tasks to be transferred to a technical solution. A risk analysis should be set up for a (generic) function including all tasks (human tasks and function of a technical system). Depending on the result, sub-functions can be shifted from the human operator to the technical system or vice versa. The overall safety can be optimised, perhaps the safety level of the system and the costs can be reduced if additional functions are included in the system.

- Normally the development of most systems (e.g. rolling stock and signalling) is a task of the suppliers. In this case a SMS is not required by the Safety Directive; SMS are only needed for RU and IM. From suppliers (no RU and no IM) the rules in the norms and other standards have to be applied. Therefore we should speak about safety management process (short: safety management) in the case of suppliers. In this way we can avoid the misunderstanding that these companies need a formal and approved SMS on the basis of the Safety Directive. It is proposed to explore a common European structure for SMS to allow the interchange of results and keep the market open.

- The Safety Directive regulates only that the safety certificate (RU) and the safety authorisation (IM) has to be renewed periodically by the Safety Authority. This is a process on a very high level that should not have any impact on the suppliers product certification or approval process.

- The text implies that first CSTs should be apportioned and then an assessment process selected based on ALARP, GAME or MEM. This is not possible! GAME or MEM themselves define risk acceptance (the same as the CSTs do). We think it can be assumed that the CSTs will be acceptable when they are introduced by the European Commission. If they would be unacceptable they should not be introduced. So the acceptability has to be proven (by one of the principles) before introduction of the CSTs.

- Generally, it must be considered that the major task (which currently poses the most problems) is the apportionment of CST to THR at a technical level (deriving safety requirements for subsystems and components). In theory, the process may look fine but practically, there is no commonly accepted solution given, neither by SAMRAIL nor by other activities or bodies such as CENELEC WG8. The challenge of ERA in this context is that the CSM must not prescribe methods which are impracticable or too expensive to implement.

- A "safety indicator related to incidents" is proposed. It has to be stated very clearly that only a certain part of incidents will be discovered.
  It is also mentioned several times that data on accidents and incidents have to be collected. But it is not clearly enough said that it has to be made the following distinction: For safety indicators (and safety targets) only data on accidents (not incidents) can be collected. For CSI we have the definition "probability of harm * severity of that harm." Because incidents do not produce harm the data on incidents can not be a contribution to the data regarding risks. Another case is to investigate the results of changes in safety rules and operational rules or of the introduction of a new system or a new technology. Here the data collected from accidents and incidents can be applied to get more significant results and to make risk related statements much earlier.

- Very specific quantitative safety targets can be obstacles for new technical solutions because remaining risks can not be shifted between sectors with different safety targets. Problems can also arise if these targets will be changed in the future (without a long transition period) and the old rolling stock and fixed installations can not meet the new safety targets. We propose safety targets on a generic level with the possibility to shift remaining risks between the different sectors (sectors can be rails and the regarding infrastructure, tunnels, bridges, signalling, telecommunication, level crossings, etc.). The mandatory safety target for a line should be accumulated by the existing (not mandatory) safety targets from the line-specific sectors. The same rules should be used for rolling stock. These proposals are in line with article 4.1 of the Safety Directive.

- It should be mentioned that the manufacturer (or supplier) should have access to the collected data (field experience data: failure data, incidents, accidents). This is a very important contribution for the manufacturer (or supplier) to set up an own learning process and to increase the safety of rolling stock, civil structures, and technical installations. Very important in this respect are data on technical reliability. This way the manufacturer (or supplier) can contribute also to the learning process of RUs and IMs.

- Regarding the independence of the assessment the proposed regulations are too restrictive and not in line with the EN 45005 and EN 45011 used elsewhere by the Commission to define inspection and acceptance bodies. The proposals can not be accepted because they are not in line with the experience in some Member States. There is no reason to make differences between "independent person", "independent department" and "independent organisation".
  In EN 50129 it is stated that the safety assessor should not belong to the same organisation as the project team, the verifier or the validator. In specific cases the assessor could be part of the same organisation as some of this parties, but other measures must then be taken to assure safety. One possible solution is a direct line of reporting between the assessor and the safety authority.
  Some Member States have very good experiences with this regulation. It should be verified whether this solution can be expanded.

- We have to be very careful when introducing new extensive assessment requirements because these may eventually lead to a cost increase in European railways without impoving the safety level. This might be useful for the safety assessors but definitely not for the competitiveness of the railway sector. The proposed assessment scheme is overly prescriptive and leaves no space to adapt for the needs of specific projects. We can find here a large number of proposed items that need checking. In our opinion the acceptable effort for safety assessment depends on the size and complexity of a project. We miss proposals to simplify the treatment of small and non-complex issues (e.g. simple changes, substitution of old components) where a large part of the described items is not required. **The risk is that too much money will be spent just to fulfil the assessment rules rather than on actually improving safety.**

The reviewed SAMRAIL reports are listed in appendix 1.

The above described and discussed items contain and summarise the main problems. The detailed comments and change requests on the reports are listed in appendix 2 as a working basis.

Appendix 1

Assessed SAMRAIL documents

No.	WP	Title of the Document	Document ID
1	2.1	D.2.1.1: Analysis of existing approaches	SAMRAIL/TIFSA/WP2.1/D.2.2.1/V4 Date 2003-10-28
2	2.2	Guidelines for the Safety Management System	SAMRAIL/SM/D2.2.2/V4.0 Date 2004-08-26
3	2.3	Report D.2.3: Common Safety Methods	SAMRAIL/ProRail-SSC/HK-PvdB/ WP2.3/V3 Date: 2004-09-21
4	2.3	(WP 2.3.1) - Framework for identifying sources, stakeholders and the nature of risks	SAMNET/LSA/PhG/WP2.3/D2.3.1/V4 Date: 2004-05-05
5	2.3	WP 2.3.2 – Common methods risk analysis	SAMTAIL/ProRail-SSC/HK-PvdB/WP2.3/D2.3.2/V1 Date: 2004-07-01
6	2.3	WP 2.3.3 – Risk Analysis Approach	SAMRAIL/TIFSA/JF/WP2.5/D.2.3.3/V4 Date: 2004-04-27
7	2.3	WP 2.3.4 – Information and Data Requirements for Risk Analysis	SAMRAIL/WP2.3.4./Contribution V1.0 Date: 2004-06-30
8	2.3	WP 2.3.4.1 – Information and Data Requirements in Risk Analysis – General Consideration	SAMRAIL//WP2.3.4./Contribution V1.0 Date: 2004-06-30
9	2.3	WP 2.3.4.2 – Information and Data Requirements in Risk Analysis – Data Sources	SAMRAIL//WP2.3.4.2/Contribution V1.0 Date: 2004-06-30
10	2.4	WP 2.4 Acceptable Risk Level	SAMRAIL/DB/PM/D.2.4/V1.0 Date 2004-06-23
11	2.4	WP 2.4.1 Definition of Risk	SAMRAIL/IfEV/GM/WP2.4/D2.4.1/V3.1 Date 2004-09-17
12	2.4	WP 4.4.2 Approaches to derivation of risk levels and risk apportionment strategies	SAMRAIL/TUD/CC/D.2.4.2/V4 Date 2004-09-16
13	2.5	D.2.5.1: Safety Approval & Cross Acceptance	SAMRAIL/SNCF/JM/WP2.5/D.2.5.1/V02 Date: 2004-09
14	2.5	D.2.5.2: Risk Based Criteria for Safety Approval	SAMNET/ATKINS/RS/WP2.5/D.2.5.2/V2 Date: 2004-06
15	2.5	D.2.5.3: Process and Mechanism for Safety Approval & Certification	SAMTAIL/TIFSA/JF/WP2.5/D.2.5.3/V4 Date: 2004-06-23
16	2.5	WP 2.5.4 – Demonstration of Compliance and Assessment Methods	SAMRAIL/DB/PM/WP2.5.4/V0.1 Date: 2004-01-04

17	2.5	WP 2.5.5 – TSI Cross-Acceptance – A case study of certification	SAMRAIL/ALSTOM/EH/WP2.5/D2.5.5/V1 Date: 2004-07-02
18	2.6	WP 2.6: Accident and incident reporting system for the EU railways	SAMRAIL/ERRI/GB/WP2.6/D.2.6.1/V2 Date 2004-07-04
19	2.7	Report D.2.7.1 Standards and Best Practice	SAMRAIL/TÜV-TIT/WP2.7/D2.7.1/V01 Date: 2004-06-22
20	2.7	Annexes to Report D.2.7.1 Standards and Best Practice	SAMRAIL/TÜV-TIT/WP2.7/D2.7.1/V01 Date: 2004-06-22
21	2.8	Regulations, roles of rules and their unification – Volume I	SAMRAIL/DTF/LL/WP2.8/D2.8.1-1 Date: 2004-06-21
22	2.8	A Framework for Safety Rule Management – Volume II	SAMRAIL/DTF/LL/WP2.8/D2.8.1-2 Date: 2004-06-21

Appendix 2

Comments and change requests on the content of the SAMRAIL Work Packages

Work Package 2.1

Nr.	Text source	Page	Comments
1	6. Findings	49 - 65	In chapter 6 "Findings" some proposals are made. The content of chapter 6 is presented in more detail in the reports on the work packages 2.2 - 2.8. Therefore we assume that the relevant SAMRAIL proposals are only to be found in the reports on the work packages 2.2 - 2.8. Nevertheless, we would like to point out that chapter 6 contains a number of questionable statements that should not be accepted. For example: • Section 6.2 provides a list of risk analysis methods from other modes of transport. The text misses conclusions drawn for the railway sector. • Section 6.3 implies that WP 2.4 provides a harmonised set of criteria methods for risk apportionment and allocation of safety integrity levels. In fact risk apportionment methods are only vaguely described and nothing is being said (neither in section 6.3 nor in WP 2.4) about the allocation of safety integrity levels. Regarding this item much more work is needed. • Section 6.3: MEM, ALARP, and GAME are not methods to derive tolerable hazard rates (THR)! They serve to define risk acceptance levels (This is something very different!). Risk acceptance levels can serve as a basis to derive THR.
2	7. Conclusions and recommendations	66 - 74	In chapter 7 "Conclusions and recommendations" some proposals are made. The recommendations are discussed in more detail in the reports on the work packages 2.2 - 2.8. Therefore we assume that the relevant SAMRAIL proposals are only to be found in the reports on the work packages 2.2 - 2.8. Nevertheless, we would like to point out that chapter 7 contains a number of questionable statements that should not be accepted. For example: • With regard to “safety targets” section 7.2 says “The author does not currently know the degree to which numerical safety targets are used in each country.”. Considering the number of companies and institutes involved in SAMRAIL it should have been possible to collect more information on this issue. Or does it mean that no or only a few numerical safety targets are used? And what are the reasons?

Work Package 2.2

Nr.	Text source	Page	Comments
1	Executive Summary No 1., line 4 and 3 Elements of SMS, No 1. line 5 and 4.1 Requirements, line 4	4 18 20	There is the sentence: *"They should be aware of their safety management responsibilities as required by Article 4.2 of the safety directive and other national requirements."* We think that the relevant article related to the explanations is Article 4.3.
2	2.2 Boundaries	13	There is the sentence: *"The entities, which are not under the control of any railway organisation, but could be sources of hazards for their operation, are identified here as boundaries."* It is not clear whether the listed entities are included in the CST, CSI etc. or not. This point should be clarified.
3	2.3 Lifecycle Stages of the Railway Transport System	14 - 15	It is not appropriate that this WP defines a specific life cycle model for the SMS, because EN 50126 contains an accepted, better defined model exactly for that purpose. It would be more appropriate to take the EN 50126 model and add additional descriptions where necessary.
4	2.3 Lifecycle Stages of the Railway Transport System, Figure 1	14	In the part "Pre-operation" are the two boxes: "System definition and application condition" and "Risk analysis and system requirements". These stages have to be supported by the developer's SMS and the "Safety plan" (right side of the figure). We think it must be explained, that the "application condition" and the "risk analysis and system requirement" must be elaborated by the RU and IM. Only these bodies can define the later application conditions of the new system and carry out a well-founded risk analysis to define the system requirements in the specific case.
5	2.3 Lifecycle Stages of the Railway Transport System, Figure 1	14	Figure 1 in section 2.3 is misleading because of the following issues: • EN 50126 covers the whole product lifecycle, not just the phases shown in the figure. • "Pre-operation" does not follow after system acceptance but starts with the system definition. • A life cycle phase covering decommissioning and disposal is missing.
6	2.4 Pre-operation, paragraph 1	14 - 15	It has to be mentioned that EN 50128 and EN 50129 only cover electrical, electronic and programmable systems. For all other areas (e.g. civil structures, mechanics, pneumatics) the standards do not provide sufficient guidance. Unfortunately, SAMRAIL does not answer the question how these areas should be managed with regard to risk assessment and how to quantify hazardous failures.
7	2.4 Pre-operation, paragraphs 1 & 2	14 - 15	There are these two sentences: *"The safety case produced for such a system must detail the developer's SMS. This SMS identifies evidence from such processes that a duty-holder can assess (See Section 9)."* Normally the development of most systems (rolling stock and infrastructure) is a task of the suppliers. In this case a SMS is not required (see safety directive); SMS are only needed for RU and IM. From developing companies (no RU and no IM) the rules in the norms and other standards have to be applied.

			The EN 50129 says regarding safety management: "*The second condition for safety acceptance which shall be satisfied is that the safety of the system, subsystem or equipment has been, and shall continue to be, managed by means of an effective safety management process, which should be consistent with the management process for RAMS described in EN 50126.*" Therefore we should speak about safety management process (short: safety management) in the case of developing companies. In this way we can avoid a misunderstanding that these companies need a formal and approved SMS. **We propose to change the above mentioned two sentences to: *"The safety case produced for such a system must detail the developer's safety management process. This safety management process identifies evidence that a duty-holder can assess (See Section 9)."***
8	2.4 Pre-operation, paragraph 4	15 - 16	There are these two sentences: *"The plans produced by the developer for operation and maintenance of their system element will need to be consistent with the approach to operation and maintenance adopted by the duty holder for their wider integrated Railway Transport System. Hence these issues should also be communicated between parties prior to handover of the system."* *"Prior to the handover"* is not sufficiently precise. These issues should be communicated as early as possible.
9	2.7 Renewal and renovations	16 - 17	This section should clearly state that each modification or introduction of safety related equipment requires to produce a risk analysis for the modification.
10	4.2.3 Sub-contracting	21	This section should mention that sub-contractors/suppliers usually require field experience data (failure data, incidents, accidents) from the duty-holder in order to be able to manage safety.
11	7.2 Generic guidance, paragraph 4	30	This paragraph should be changed to: *"Where third parties (e.g. sub-contractors) or bodies (inhouse safety assessors) in line with EN 50128 (6.2.10) and 50129 (5.3.9) are employed to undertake roles within the scope of the duty holder's business (See Section 4) then arrangements should be in place to ensure that the organisation can enforce the same degree of competence and fitness management upon these parties as would be deemed necessary for employees within the organisation itself (See Section 9)."*
12	8.2.2.1 Internal risks and 8.2.2.5 Risk at the transition between lifecycle phases	32 33	It has to be clarified what "equipment" means. Without a definition it is not clear that rolling stock and also civil structures are included in "equipment". Alternatively other terms than "equipment" should be used.
13	9.2 Generic Guiance, paragraph 3 (There are ….. work activity)	36	In line with comment Nr. 14 the formulation in this paragraph should be changed to avoid the term SMS because the suppliers do not have to have a safety management system but a safety management process. For equipment related to the EN 50129 in the safety case has to be shown that the safety management process fulfils all requirements in a specific case.
14	9.2.1 Sub-contractor Management	37	There has to be made a clear distinction between • railway undertakings (RU) / infrastructure managers (IM) and • sub-contractors (e.g. suppliers, engineering companies and other service providers). Only the safety management of the first group needs a certificate (Safety Directive Art. 10 (2) a) and Art. 11 (1) a)). For the second group the EN 50126 (and additionally EN

			50128 / EN 50129 where applicable) with the rules related to the safety management process have to be applied. If sub-contrators (especially suppliers) can show that the safety management process is part of the approved safety case for systems, sub-systems or components no additional considerations and examinations by the RU / IM are required.
15	9.2.2.1 Product and equipment assurance	37 - 38	In this part of the report it should be discussed how a risk analysis approach could be defined for systems like civil structures. Not only the rules in EN 50126 - EN 50129 have to be seen in this context (see also comment Nr. 6).
16	9.2.2.1 Product and equipment assurance, paragraph 2	38	There is the last sentence: *"The ultimate requirement is that the duty-holder should assure themselves that the equipment will meet the appropriate risk assessment criteria in its proposed application."* It is very important to say that this way is only possible when the duty-holder at the beginning of the development has specified all requirements for the new system or component.

Work Package 2.3

Nr.	Text source	Page	Comments
1	Report 2.3: Document Abstract, last paragraph	2	This paragraph says: *A first set of CSMs, covering at least the "risk evaluation and assessment method" shall be developed and adopted by 2006. […]* This sentence does not seem to be in line with the new Safety Directive: *"Article 6* *Common safety methods* *1. A first set of CSMs, covering at least the methods described in paragraph 3(a), shall be adopted by the Commission, before (Four years after the entry into force of this Directive, that is 30.04.2008), in accordance with the procedure referred to in Article 27(2). They shall be published in the Official Journal of the European Union.* *A second set of CSMs, covering the remaining part of the methods as described in paragraph 3, shall be adopted by the Commission before (Six years after the entry into force of this Directive; that is 30.04.2010), in accordance with the procedure referred to in Article 27(2). […]."* There is more time than written in the report. We think the whole railway sector should be very careful with new CSM. Regarding the TSIs we can see how much time it takes to set up new rules. Our message is: Quality first!
2	Report 2.3: Executive summary, paragraph 4, sentence 1	5	See comment 1.
3	Report 2.3: 1.3. Scope of this document, bullet point 1.	13	This point says: "*The perspective that the European railways have met an acceptable level of safety; the principle implicates that new railways built according to existing specifications are safe enough. This is expressed is principles like GAME and MEM."* We think only GAME is related to the content of the sentence. The "definition" of the MEM principle is not to compare the safety level of a new system with the levels of present systems.
4	Report 2.3: 1.3. Scope of this document, bullet point 4.	13	This point says: *"[…]. To make the industry competitive with other modalities of transport the level of safety has to be improved continuously but not at any price and in an economically accountable way. […]."* Improving safety is no factor to make the railway industry more competitive with other modes of transport. As mentioned in other chapters and other WP reports, the railway system already is very safe and improvements may be valuable but not necessarily required.
5	Report 2.4: 4. Common process of risk management	19 - 25	*"[…] however, on the basis of principles like ALARP continuous improvement of the process (i.e. the level of safety) is a necessity."* This statement is wrong, ALARP does not require continuous improvement. It only requires to repeatedly assess the practicability of reducing risks (see also comment no. 4 above). What is the aim of this section? The introduction mentions

			some steps of the risk management process but does not provide any details about these steps. The following subsections 4.1 - 4.7 are about specific aspects of risk management but there is no process description.
6	Report 2.4 4.1 Bowtie–model	19 - 21	The stages listed in bullet points are not consistent: It obviously does not make sense that “Risk Management” is one of the six stages of “Risk (based) Management”. It is misleading that SAMRAIL describes a separate risk management process because such a process is already described in EN 50126. If it is really deemed necessary to describe the process, at least the same terms should be used.
7	Report 2.4: 4.2 Risk Matrix	21	The description of the risk matrix is misleading. In order to assess risk, consequences and frequency of those consequences must be used. It is wrong to assess accident severities (hazard consequences) alongside hazard frequencies. The reason is that a hazard does not always lead to an accident (i.e. the consequence assumed). The probability that a hazard (e.g. brake system failure) results in an accident (e.g. collision) can be very different (between almost 0% and 100%) and must not be neglected. There is no basis for the risk levels given in the table. EN 50126 only gives an example, while the report implies that the given matrix is an accepted risk acceptance method from the standard. It must be added that figure 1-1 is only an example for a risk matrix. What is the relationship between the matrix and the CSTs? The text says “Such a matrix could be the result of a qualitative analysis and evaluation of risks.” What is the use of the matrix, if no relationship to the CSTs can be made up? When is it sufficient to undertake a qualitative risk assessment instead of a quantitative analysis based on CSTs? This should be clarified.
8	Report 2.3: 4.5 Risk evaluation and 4.6 Risk reduction	23 - 24	The section contains the following sentences: *In order to evaluate the derived risk(level)s they have to be compared with the CSTs (or with other national legislation and/or requirements) [paragraph 2].* *[…]. This THR can be considered as a measure of the maximum acceptable rate of occurrence of a particular hazard […]. In this way the assessment of risks is in accordance with principle of CSTs as stated in the European Safety Directive.* As we understand the process the CSTs have to be compared with the remaining risk after risk reduction. By applying risk reduction measures an unacceptable risk can be reduced to an acceptable level. This is not shown in the report. The text implies that first CSTs should be apportioned and then an assessment should be made based on ALARP, GAME or MEM. This is not possible! GAME or MEM themselves define risk acceptance (the same as the CSTs do). We think it can be assumed that the CSTs will be acceptable when they are introduced by the European Commission. If they would be unacceptable they should not be introduced. So the acceptability has to be proven before introduction. Generally, it must be considered that the major task (which currently poses the most problems) is the apportionment of CST to THR at a technical level (deriving safety requirements

			for subsystems and components). In theory, the process may look fine but practically, there is no commonly accepted solution given, neither by SAMRAIL nor by other activities or bodies such as CENELEC WG8 (application guide of EN 50126). The challenge of ERA in this context is that the CSM must not prescribe methods which are impracticable or too expensive to implement.
9	Report 2.3: Tables 4-1 and 4-2	23 - 24	The role and the benefit of these tables is not clear. We have risk evaluation and risk reduction leading to quantitative results. These results have to be compared with the regarding CST (and perhaps CSIs). What is the aim of these tables? What is the rationale behind the tables 4-1 and 4-2? The tables are **examples** from EN 50126. On which basis does SAMRAIL define that the tables represent appropriate risk acceptance criteria? The use of the risk matrix can only make sense if it is first calibrated on the basis of the future CSTs. Then it could in fact become an alternative to quantitative methods. If this is the intention of the SAMRAIL authors this process should be clearly described.
10	Report 2.3: Tables 4-1	23	Three times the abbreviation RA is mentioned. What does it mean? Railway Safety Authority (RSA) or Railway Undertaking (RU) or Infrastructure Manager (IM)?
11	Report 2.3: 4.5 Risk evaluation	24	Sometimes in the document the abbreviation THR is used in a wrong way: It has to be very carefully distinguished between HR (before the comparison with the safety target) and THR (after the comparison with safety target and if it is really tolerable).
12	Report 2.3: 6 Common Risk Controls	27	The fourth bullet point says: *Correction of events or situation;* *When human errors are made, like signals passed at danger (SPAD) or in case of system failure, corrective measures can be installed. For instance, if a train driver makes a SPAD, automatic train protection systems can take control of the train and perform an emergency brake to prevent the top event from happening. If a technical system fails it can be made fail-safe so that it can only fail in such a manner that no unsafe situations can occur.* The last underlined sentence is not always true. Today, very often new signalling system are developed on the basis of EN 50129. There remains a minimum part of risk coming from technical installation; also in the case of fail-safe development. Safety is not absolute.
13	Report 2.3: Appendix A4	2	The first sentence says: *The MEM principle is practiced in Germany and has been derived […].* The sentence is not fully correct. In the railway industry the EBO (German railway regulation) is applied. The general regulation in EBO is very similar to the GAME principle. MEM is only applied in very special cases and sometimes additionally to verify the results coming from GAME. But it is not used in the official German railway acceptance/certification process.
14	Report 2.3.1: 7.4 Conclusion: scenarios proposed for the framework	25 - 36	The scenario list is not helpful. In particular, it is far too detailed. EN 50129 says “Methodologies which generate an unrealistic large number of mostly trivial or imprecisely defined hazards are wasteful of resource and can lead to a misleading or unproductive risk assessment. With the exception or large undertakings, involving many personnel, activities and equipment, a large list of hazards extending into the hundreds is unreasonable and indicative of a poorly designed or con-

			ducted study.“. The list of WP2.3.1 has more than 600 items! Still it is incomplete (on that level of detail completeness is impossible, for example: The cause for a "Station buffer collision" (4.5.1.2) can also be a "Signal failure" as listed under 4.5.1.1.1.2.3.2 and 4.5.1.3.1.2.3.2). It is ambiguous, inconsistent and not generic.
15	Report 2.3.2: chapters 3.2.3 – 3.2.5	8 - 9	See comments 9.
16	Report 2.3.2: Appendix A4		With regard to “SIL classification” it has to be said that this process is not fully in line with EN 50126 and 50129. With regard to SIL classification it says: *“This method analyses a hazard or potential dangerous situation in order to assess the risk, resulting in a certain Safety Integrity Level (SIL).”* This statement is misleading. Please refer to EN 50126 and EN 50129 which describe the safety integrity concept. Furthermore it says: “*For instance SIL 2 reduces the risk with a factor 10^2.*” This statement is misleading because it is related only to the “low demand mode” mentioned in IEC 61508. The railway signalling standard EN 50129 however does not use this definition.
17	Report 2.3.3:	all	We like to stress our comments on report 2.3. This report 2.3.3 is (in our understanding) only a contribution to report 2.3 and not a separate and independent document. Report 2.3 has assessed this report. Items not mentioned in report 2.3 are in our understanding not relevant.
18	Report 2.3.3: 1.1 Definitions	4 - 5	The definitions are not totally identical with those in the new Safety Directive and the European standards (EN). The definitions in those documents should be respected precisely. Generally, the source of the definitions should be given.
19	Report 2.3.3: 2.1 Risk reduction	5 - 7	Here only the ALARP principle is mentioned. But there are other principles, as shown in report 2.3.
20	Report 2.3.3: 2.3 Design of safety systems	8 - 12	In this chapter only the means regarding safety systems are described. But what about systems (outside the scope of safety systems) producing incidents and perhaps accidents in the case of faults (track infrastructure, energy and rolling stock)?
21	Report 2.3.3: 2.3.2 Automation strategy	12	Automation means to shift tasks from the human operator to technical systems. It should be mentioned that risk analyses could give answers. A risk analysis should be set up for a (generic) function including all tasks (human tasks and function of a technical system). Depending on the result, subfunctions can be shifted from the human operator to the technical system or v.v. The overall safety can be optimized, perhaps the safety level of the system and the costs can be reduced if additional functions are included in the system.
22	Report 2.3.4.1: 4.7 Data for failure of software, paragraph 2	8	There is the sentence: ”*As a result data for failure of software is not obviously at hand, only the figure of software releases can gave an indication about the number of modifications.”* This statement is misleading. The number of software modifications is not a meaningful parameter for the derivation of failure data (not all software modifications are caused by failures). Very often the functional requirements change which may as well require a software modification.
23	Report 2.3.4.1: 6.1 Expert Judgement versus Engineering Judgement	10 - 11	This chapter and especially table 1 gives a picture in black and white. In practical work the judgement is carried out in a kind of mix of formal and expert judgement. But this way is not described.

24	Report 2.3.4.2:	all	This document contains an analysis and one aims to facilitate the identification of data defined within the scope of European Railway directives and standards which could be useful for the Common Process of Risk Analysis. An amount of data including the "cross dependencies" between the different sources (and references) is listed. There are no clear proposal for the work in the future. So it is not required to give comments (in detail).

Work Package 2.4

Nr.	Text source	Page	Comments
1	WP2.4/ 1. Introduction	6	The target *"propose an approach to establish quantitative and qualitative risk levels for the community railway systems and their components, including allocation of SIL, risk apportionment strategies"* has not been reached. The SAMRAIL reports are only a contribution to this target but still far away from being a consistent and practicable solution to this problem.
2	WP 2.4 / 3.2. CST – Definitions and Interpretation (second paragraph)	9	The reference "(Article 3)" has to be changed to "(Article 7, paragraph 4)".
3	WP 2.4 / 3.2. CST – Definitions and Interpretation (last paragraph)	10	The reference "(Article 7)" has to be changed to "(Article 8)".
4	WP 2.4 / 3.3. Objectives of CSTs (first paragraph)	10	The reference "(Article 7)" has to be changed to "(Article 8)".
5	WP2.4 / 3.3 Objectives of CSTs (paragraph 3)	10	The definition of "safe transport process" is not very suitable. A risk-related definition should be used. Suggestion: "Transport of people or goods by a rail-guided mode of transport from a location to its destination (including loading and unloading) without exceeding the accepted risk level."
6	WP 2.4 / 3.4.2 Global CSTs	13	The report is inconclusive: What is the proposal for CST: the average, the median or the upper 25% performance?
7	WP2.4 / 4.1 Definition of risk	14	The discussion of the definition of risk focuses too much on definitions used in computer applications. This is not the appropriate level for the top level discussion. Many societal aspects e.g. risk aversion have not been taken into account as well as basic publications as ISO (2001). Risk Management – Vocabulary – Guidelines for Use in Standards, Guide 73.
8	WP 2.4 / 4.2.3. Tolerable risk	16	Basic facts from accident analysis (e.g. reason) are not acknowledged, e.g. that the majority of accidents does not have technical root causes but organisational. Technical root causes are exceptional. However organisational causes are not taken into account by technical standards, e.g. EN 50126 or EN 50129. So there is a very sparse (if any) statistical bases for setting tolerable risk levels for technical systems.
9	WP 2.4 / 4.4. Reference units (paragraph 7)	18	The second sentence in paragraph 7 says: "*It can be transferred to most of the other definitions in use. For the consideration of individual risk of fatality it is necessary that values for average speed and average number of people on a train have to be collected.*" We have to say very clearly, that the values for "average speed" and "average number of people on a train" are derived values. They can not be very precise so that we propose to use only the value "personal damages [equivalent fatalities] / train running distance [trainkilometer]". If some Member States like to use for internal reasons the other values they can do it. But on European level (e.g. statistics and cross acceptance) only "personal damages / train running distance" should be used.
10	WP2.4 / 5.1 ALARP	20	ALARP is practised in much more countries, e.g. Switzerland, and in many different ways.
11	WP2.4 / 5.1 MGS-Principle	20	Discussion of MGS is over-simplified. It is not true that any existing system would do for comparison. And FBO is not the

			existing system would do for comparison. And EBO is not the only applicable law with regard to product safety in Germany, so there come additional legal duties from other sources.
12	WP 2.4 / 5.4 MEM, 2nd paragraph	20	Delete "new" because MEM is applicable not only to new systems.
13	WP 2.4 / 5.4 MEM, last sentence	21	The statement that MEM is not applied yet in railways is not fully correct. To be changed to: "The MEM-principle is often referred to as the German principle but it is not used in the official German railway acceptance/certification process. In railways, it has been applied in a number of projects for non-official risk analyses or additional analyses."
14	WP2.4 / 5.4 MEM	21	The discussion on MEM is not correct. The original source (Kuhlmann) states, that the tolerable risk from all transport systems may be 1E-8/hour per individual. Given that in one particular hour an individual is only exposed to railways this would be the appropriate MEM target. But the report sets a much more demanding target! Why?
15	WP 2.4 / 5.5 Conclusion for Acceptance Criteria	21	We recommend an addition to this section (5.5): "The application of the MEM principle does not require the existence of statistical data on the actual safety performance. Instead, it is based on a postulate and requires an agreement between the involved stakeholders. Therefore, the application of MEM might be useful in exceptional cases, e.g. when the application of other quantitative risk criteria is not possible or too complex. It can also be used to verify CST."
16	WP 2.4 / 6.1. Level of Specific CSTs (paragraph 3)	22	There are these two sentences: *"The degree of responsibility for each organisation is also likely to show significant variations depending on the railway systems used in every Member State, thus reaching an agreement on CSTs at this level would be problematic. However it is believed that at a level below that of the CSTs, when SILs and failure rates have been defined for some particular protection functions and their physical constituents, only then it should be possible to allocate responsibilities between IM and RU, but this would have to be done on a case by case basis depending on the specific application."* So far SIL only have been defined for electric, electronic and programmable systems. For all other technology (e.g. mechanics, pneumatics, hydraulics) the safety integrity concept has not been specified and thus it is difficult to apply. Generally, it should be discussed whether it is reasonable at all to apply the safety integrity concept to all parts of the railway system. In this regard it should be mentioned that it will be very hard to define CSTs and SILs for civil structures and many other parts of the railway system. There are no norms and no standards regarding the derivation of values for CSTs and SILs depending on the kind of construction of, e.g., a bridge, a tunnel, a cut, and other civil structures. This problem is not mentioned in the whole report. But the problem stands in front of us.
17	WP 2.4 / 6.1. Level of Specific CSTs (paragraph 4)	23	There are the following sentences: *"For instance, if a common global target was to be set per passenger*km, then for those countries preferring to use passenger*hours as a reference value this would mean automatically, by conversion, a different target for high speed and conventional lines. If those countries were internally not to accept this on the grounds mentioned above, they might then want to set different spe-*

			*cific targets per passenger*km for high speed and conventional lines on their territory in order to have an equal target on both types of lines as measured per passenger*hours."* This problem can and should be avoided by using only one safety target for both high speed and conventional lines (value: personal damages / train running distance).
18	WP 2.4 / 6.1. Level of Specific CSTs (paragraph 6)	23	There are the following sentences: *"It is clear that setting common targets for components, processes or hazards which are too specific of a particular railway system will not be sensible, unless the system being considered or to be designed happens to be common in all Member States, as is planned with ERTMS for instance. It is thus felt that as a condition for setting specific CSTs, one should stop short of technical aspects and specific incarnations of the railway system, so as to remain sufficiently generic, and yet provide also some common criteria for safety that could be used for interoperability and cross-acceptance purposes."* We like to underpin these sentences. Very specific safety targets can be obstacles for new technical solutions because remaining risks can not be shifted between sectors with different safety targets. Problems can also arise if these targets will be changed in the future and the old rolling stock and fix installations can not meet the new safety targets. Another problem is not discussed in the report. If there are specific safety targets for components and small systems, the amount of these components (e.g. point machines) and small system (e.g. level crossing systems) on a line will define the safety level of the line. In other words: We propose safety targets on a generic level with the possibility to shift remaining risks between the different sectors (sectors can be rails and the regarding infrastructure, tunnels, bridges, signalling, telecommunication, level crossings, etc.). The mandatory safety target for a line should be accumulated by the existing (not mandatory) safety targets from the line-specific sectors. The same rules should be used on the side of rolling stock.
19	WP 2.4 / 6.2. Risk Apportionment Strategies (figures 2, 3, 5, 6 and the regarding text)	24 - 27	In the figures and the regarding text there is not mentioned that the hazards not only result from technical problems. The human factor (operator, driver etc.) plays a very important role. It can be (especially in degraded modes) that in some cases the resulting safety is determined by the human factor and not so much by failures on the technical side. These facts should be considered in this chapter. With regard to the influence of the human factor on the resulting safety it should be discussed what the influence of the availability of the technical part of the railway system on the resulting safety is. In many cases the human factor plays in the time of the non-availability of an item (component or subsystem or system) the main role for the resulting safety of the railway system (depending on the item and the operational rules).
20	WP 2.4 / 6.2. Risk Apportionment Strategies	24	While figure 2 has shown to be well applicable to mainly electronic systems, it has not been applied to other systems, e.g. mechanical and especially civil construction. It is not even clear that the key concepts, e.g. THR, are applicable in other

			domains. What is the justification for this approach? See also other comments on the same problem!
21	WP 2.4 / 6.2 Risk Apportionment Strategies, figure 6	26	The figure implies that there is an unequivocal (one-to-one) relation between hazard and risk. This simplification does not match reality. Some cross connection should be added to emphasize the complexity.
22	WP 2.4 / 6.2. Risk Apportionmant Strategies (last paragraph)	27	There are the following sentences: *"Thus it is important to stress that whichever way the risks might be apportioned for defining CSTs, there will still be some rather complicated safety allocation process necessary behind, in order to derive (qualitative and quantitative) safety requirements […]. Specific CSTs could nevertheless serve as useful quantitative reference values in this process. Whether this process could then be conducted at a EU level in order to achieve common safety requirements for the EU railways down to each constituent remains an open question, due to the huge difficulty of the task."* See our above comments on 6.1. Level of Specific CSTs (paragraph 6).
23	WP 2.4 / 7.2. Functional breakdown (table 3)	30	Apparently, the AEIF-List of functions has been set up for purpose of interoperability. This is not compatible with the life cycle oriented CENELEC view. This raises the question how the safety target for e.g. civil constructions, rolling stock and signalling can be derived because the safety target of an item is involved in more than one of the mentioned functions.
24	WP 2.4 / 7.2. Functional breakdown (paragraph 4)	30	There is the following sentence: *"Using the "Railway Architecture" of AEIF it will be necessary by carrying out a hazard analysis to identify for each defined function the related hazards (due to malfunction) and its resulting type of accident."* See our above comments on 6.2. Risk Apportionmant Strategies (figures 2, 3, 5, 6 and the regarding text).
25	WP 2.4 / 7.2 Functional breakdown, footnote 5	30	Plural should be used: There is hardly any accident that was caused be exactly one single failure.
26	WP 2.4 / 7.3, 2nd paragraph	32	In the sentence "Therefore, safety targets for a considered function can be derived by calculating the contribution..." the word "calculating" should be replaced by "estimating". "Calculating" misleads to a non-existent precision.
27	WP 2.4 / 7.3. Apportionment of Global CSTs (figure 9)	32	Figure 9 shows a solution for a breakdown of accidents related to functions. Such a breakdown can lead to very detailed CSTs and CSIs. This makes sense to identify functions with an unacceptable high risk level where the risk has to be reduced. But it is a problematic way to set up mandatory safety targets on this level. See also our comments on 6.1. Level of Specific CSTs (paragraph 6).
28	WP 2.4 / 7.4. Demands on CSIs (last paragraph)	33	The content of this paragraph seems to lead to a change of the annex of the Safety Directive.
29	WP 2.4 / 7.6. Interoperability (paragraph 1)	34	The last sentence says: "*Also for new technologies and products, for which no technical standard exists anywhere, specific CSTs would be useful in providing common risk acceptance criteria to be applied in the acceptance and cross-acceptance procedure.*" This statement is rather questionable because it implies that the need for CSTs is not eminent if there are technical standards existing. The problem with this statement is that compliance with technical standards is usually **not** sufficient to derive quantitative risk values. It is necessary to adhere to technical standards (if existing) but this is usually not sufficient to demonstrate safety. Following the CENELEC safety management approach, safety requirements are necessary for **all**

			functions and components. This is well described in another section of the WP2.4 report: it is a long way from the provision of CSTs to the apportionment of these targets to requirements for functions and components.
30	WP 2.4.1 (whole report)	all	This report was evaluated. Comments are only given if there is no comment on this item in the comments on report 2.4.
31	WP 2.4.1 / 3.1 Incident and accident (Paragraph 1, definitions)	16	The reference "(i)" has to be changed to "(k)". The old reference (k) has to be changed in the following way: *(l) "serious accident" means any train collision or derailment of trains, resulting in the death of at least one person or serious injuries to five or more persons or extensive damage to rolling stock, the infrastructure or the environment, and any other similar accident with an obvious impact on railway safety regulation or the management of safety; "extensive damage" means damage that can immediately be assessed by the investigating body to cost at least EUR 2 million in total;* *(m) "incident" means any occurrence, other than accident or serious accident, associated with the operation of trains and affecting the safety of operation;*
32	WP 2.4.1 / 3.1 Incident and accident (Table 3-1)	19	The definition of "serious accident" is not in line with the definition in the final version of the Safety Directive (see the above comment).
33	WP 2.4.1 / 4.2 Statement of National laws)	28 - 30	In this chapter only the paragraphs regarding Germany (4.2.1) have been assessed by the VDB.
34	WP 2.4.1 / 5.4 MEM	32	The statement that MEM "has not been used in railway safety assessments" is not fully correct. To be changed to: "The MEM-principle has not been used yet as part of an official railway acceptance/certification process. It has been applied in a number of projects for "non-official" risk analyses or additional analyses."
35	WP 2.4.1 / 6.3.2 Normal operation and operation in situations of degraded service	39	We like to underpin this paragraph because the relation between availability and the resulting safety is a very important issue. In the discussions about safety in the last decades the influence of the human factor during the time of degraded modes was not seen in the clear light. In signalling the resulting safety can be upgraded by an upgraded availability (see also our comment in WP 2.4 / 6.2. Risk Apportionmant Strategies (figures 2, 3, 5, 6 and the regarding text)).
36	WP 2.4.2 (whole report)	all	This report was evaluated. Comments are only given if there is no comment on this item in the comments on report 2.4.
37	WP 2.4.2 / 3.1 Safety Directive Requirements (paragraph 4)	7	The reference "(7)" has to be changed to "(8)".
38	WP 2.4.2 / 4.2 System breakdown, approach a) (paragraph 4, third bullet point)	16	This sentence says: "*The distribution of risks according to constituent parts should not be "frozen" and would thus require frequent updating in order to keep track with changes in the technology.*" The message of this sentence is clear, but behind it many problem can arise, e.g.: • What will happen with the older technical solutions when new safety targets shall be introduced? • What happens with the safety targets on a higher level when constituents with new and old safety targets are combined in operation which may lead in result to a higher risk? • What happens when one RU or IM likes to introduce new technology with other safety levels and the safety targets would not be changed?

			We fear that safety targets on a low level will reduce the flexibility of RUs and IMs to change technology. And this will hinder the revitalising of the European railway system.
39	WP 2.4.2 / 4.5, figure 5	19	The figure implies that there is an unequivocal (one-to-one) relation between hazard and risk. This simplification does not match reality. Some cross connection should be added to emphasize the complexity (see comment on WP 2.4 above).

Work Package 2.5

No	Text source	Page	Comments
1	Report 2.5.1: 3.1 Definitions and Acronyms	6 - 7	The assessment is an important part of the process as defined in e.g. EN 50128 and EN 50129. It should be added, because in chapters 3.2.1 assessment reports are mentioned. Safety certification is defined as: *[….] performed independently from the seeker by a publicly accredited organisation, which by using objective evidence, […].* It is not required to have an organisation. Also persons can perform the task. So the definition should be changed to: *[….] performed independently from the seeker by a publicly accredited organisation and/or person, which by using objective evidence, […].* *Cross acceptance: The status achieved by a product […].* This definition is in line with the EN, but in the daily work cross acceptance is used for the process to accept a product which was already accepted by another body. So cross acceptance needs a new definition. For the present definition the term cross acceptability should be used. "Safety approval" and "Safety acceptance": See comment 5, bullet point 3.
2	Report 2.5.1: 3.2.2 Summary board of stakeholders for National Safety Approval processes	9	The table has 5 rows with the title "Germany". Some of the contributions in the boxes are not correct. Due to the fact, that this is not important for new European regulations, we omit to provide detailed comments.
3	Report 2.5.1: 5.1 Scope and purpose of the proposal	22 - 23	The first paragraph on page 23 includes the following sentence: *"It is important to highlight that the process which will be defined is a generic process for certification."* We like to stress this statement. It should be expressed that from the four possible application levels only the levels 1 and 2 are relevant for the supplier. On level 3 the regarding assets can come from different suppliers. So RUs and IMs are the main actors. In specific cases the RU and/or the IM can be supported by the suppliers. Therefore the comments only regard those cases in which the suppliers are concerned.
4	Report 2.5.1: 5.3.1 Introduction and presentation, paragraph 2	26	See comment 5.
5	Report 2.5.1: 5.3.1.2 Actors and roles	27	As we understand the final version of the Safety Directive and the Directives 96/48/EC and 2001/16/EC regarding interoperability some items in this chapter are not in line with the Directives: • Bullet point 1: Requesting entity: The Safety Authority is no requesting entity (see the comments regarding bullet point....). It has to be deleted. • Bullet point 2: This bullet point should get the label "Certification / Safety Assessment Entity" In the case of assets under the regulation of the directives

			96/48/EC and 2001/16/EC this is a task of "Notified Bodies" in the sense of these directives. Under conditions they can have sub contracts with other bodies. In the case of assets <u>not</u> under the regulation of the directives 96/48/EC and 2001/16/EC this task can be performed by -- accepted organizations and -- accepted persons (e.g. Independent Safety Assessors) as well as -- Notified Bodies in the above mentioned sense. • <u>Bullet point 3:</u> In the Safety Directive IMs and RUs are no approving entities. They can accept certificates from the notified organisations or accepted bodies and person (see bullet point 3) and present it to the safety authority or not. Internal decisions of the railway should not have the label "approving". This bullet point has to be deleted. • <u>Bullet points 4 and 5:</u> There are no different roles for Safety Authorities and the Ministry of Tansport. The Safety Directive says: *"Each Member State shall establish a safety authority. This authority may be the Ministry responsible for transport matters and shall be independent in its organisation, legal structure and decision making from any railway undertaking, infrastructure manager, applicant and procurement entity."* That means that the tasks mentioned in § 16 (2) can be carried out in some Member States by the safety authority and in other Member States by the ministry of transport. The authorisation to put some thing in service is no specific task of the ministry. Therefore the two bullet points should be merged and get the label "Approving and authorising entity (Safety Authority or Ministry of Tansport)". The tasks should be described as -- Safety approval, -- Authorising for the put in service. • <u>Bullet points 6:</u> Others: The first line (Independent […..] Approvers) should be deleted (reason see above).
6	<u>Report 2.5.1:</u> 5.3.1.3 Regulatory framework proposed by the Standards EN 50126, EN 50128 and EN 50129 and 5.3.2 Proposal for a Safety approval & certification process	27 - 29	In these chapters often the term "verification of conformity" is used. That is right in many of the cases and should not be changed. But doubts can arise in the case of the certification process for an asset like a technical system, sub system or component. Therefore for these cases in parallel the term "assessment" (see EN 50126, 50128, 50129) should be used. This addition is important to avoid misunderstandings.
7	<u>Report 2.5.1:</u> 5.3.2.1 Seek and 5.3.2.2 Analysis and test	29 - 30	Always only “Notified Body” is mentioned. Please also consider bullet point 2 in comment 5 (accepted organizations and accepted persons).
8	<u>Report 2.5.1:</u> 5.3.2.2 Analysis and test	30	Only the term “certification process” is used. Please also consider comment 6 regarding “assessment”.
9	Report 2.5.1: 5.3.2.3 Decision	30	Paragraph 3 includes the following sentence: *In this moment, the certificate will be sent to the requesting*

			entity with a period of validity of five (5) years, […] In the report is not clearly expressed that this sentence is not valid for technical products of the suppliers; it is only valid for the items listed in the Safety Directive. This Directive says: *Article 10 - Safety certificates* *1. In order to be granted access to the railway infrastructure, a railway undertaking must hold a safety certificate as provided for in this Chapter. […].* *2. The safety certificate shall comprise:* *(a) certification confirming acceptance of the railway undertaking's safety management system as described in Article 9 and Annex III, and* *(b) certification confirming acceptance of the provisions adopted by the railway undertaking to meet specific requirements necessary for the safe operation of the relevant network. The requirements may include application of TSIs and national safety rules, acceptance of staff's certificates and authorisation to place in service the rolling stock used by the railway undertaking. The certification shall be based on documentation submitted by the railway undertaking as described in Annex IV. […].* *5. The safety certificate shall be renewed upon application by the railway undertaking at intervals not exceeding five years. It shall be wholly or partly updated whenever the type or extent of the operation is substantially altered. […]* *Article 11 - Safety authorisation of infrastructure manag*ers *1. In order to be allowed to manage and operate a rail infrastructure the infrastructure manager must obtain a safety authorisation from the safety authority in the Member State where he is established.* *The safety authorisation shall comprise:* *(a) authorisation confirming acceptance of the infrastructure manager's safety management system as described in Article 9 and Annex III, and* *(b) authorisation confirming acceptance of the provisions of the infrastructure manager to meet specific requirements necessary for the safe design, maintenance and operation of the railway infrastructure including, where appropriate, the maintenance and operation of the traffic control and signalling system.* *2. The safety authorisation shall be renewed upon application by the infrastructure manager at intervals not exceeding five years. It shall be wholly or partly updated whenever substantial changes are made to the infrastructure, signalling or energy supply or to the principles of ist operation and maintenance. […].* Article 10 addresses the RU and article 11 the IM, but not the suppliers / manufacturers. Items of the certificate (valid for 5 years) are in both cases – the SMS of the RU / IM and – the provisions of the RU / IM to meet specific requirements.

			We propose to make this facts very clear in the report.
10	Report 2.5.1: 5.3.2.3 Decision	30 - 31	The term “certification report” is used. Please also consider comment 6 regarding “assessment”. Additionally see comment 7.
11	Report 2.5.1: 5.3.2.3 Decision	30 - 31	In bullet point 1 and 2 we can find the following parts in the sentences: [...] *the RU or the IM, can approve the asset,* [....] and [...] *the RU or the IM, can perform the approval of the asset,* [....]. See bullet points 4 and 5 in comment 5.
12	Report 2.5.1: 5.3.2.3 Decision	30	Paragraph 4 includes the following sentence: *”In the case where the requesting entity is the supplier or the railway industry, and they receive the requested certificate, they can provide the asset and the corresponding certificate to the RU or IM which hired them.”* The supplier should not be obliged to send the original certificate but only a copy of the certificate. In the case of generic products and generic applications one certificate or assessment report is needed several times.
13	Report 2.5.1: Figure n°1A	32	At the top there is a box with the inserted text "Seek (7.2.1)". It has to be changed to "Seek (5.3.2.1)". At the left side there is a box with the inserted text "Notified Organisation). See comment 7. At the left side there is a box with the inserted text "Subsystem approval). See bullet points 4 and 5 in comment 5.
14	Report 2.5.1: 5.3.2.4 Complaint and certificate suspension	32 - 33	The term “certification process” is used. Please consider comment 6 regarding “assessment”. Additionally see comment 7.
15	Report 2.5.1: Figure n°1B	34	At the top there are two boxes with the inserted text parts "(7.2.4)" and “(7.2.5)”. These have to be changed to "(5.3.2.4)" and "(5.3.2.5)". At the left side there is a box with the inserted text "Notified Organisation). See comment 7.
16	Report 2.5.1: 5.3.2.5 Maintenance of the certificate	34	See comment 7. If the certificate has to be renewed, the process runs to connector D (in figure n°1B). That means, the whole certification process has to be performed once more. This is not appropriate. Two cases should be distinguished: • The asset was not changed since the previous certification. A very simple process should be triggered to verify whether the requirements have changed dramatically in the mean time. Only in this case a simplified process should be triggered. • The asset was changed since the previous certification. Then a simplified process should be triggered to verify only the consequences of the changes. In the Safety Directive regulates only that the safety certificate (RU) and the safety authorisation (IM) has to be renewed periodically by the Safety Authority. Regarding chapter 5.1 this is a process on a very high level (not levels 1 and 2, perhaps level 4). Therefore the suppliers propose, that their certifications regarding systems, sub systems and components have not to be periodically renewed. In this case bullet point 1 can be deleted.
17	Report 2.5.1: 5.3.2.5 Maintenance of the	34	This chapter of the report describes that the notified body has to perform some tasks. That is not right. The Safety Directive

	certificate		(in the final version) does not mention notified bodies. It is the task of the Safety Authority.
18	Report 2.5.1: 5.3.2.6 Process follow up	35	It is not defined when the follow up is started. This should be added (no connector in figure n°1C). See comment 7.
19	Report 2.5.1: Figure n°1C	36	At the top there is a box with the inserted text parts "(7.2.6)". This has to be changed to "(5.3.2.6)". At the left side there is a box with the inserted text "Notified Organisation). See comment 7.
20	Report 2.5.1: 5.3.3.1 Seek and audit and 5.3.3.2 Demand of a specific safety certificates	37 - 39	See comment 7.
21	Report 2.5.1: 5.3.3.3 Decision and 5.3.3.4 Authorisation for service (opening the line)	39	The last paragraph in chapter 5.3.3.4 says: *"In the case where the safety authority belongs to the Ministry of transport, the sub-process 7.3.3 and 7.3.4 could be joined and understood as a single activity. In this situation, the safety acceptance and the authorization for the service will be achieved in one step."* That is right. But in the case that there is a safety authority (normal case) the Safety Directive determines that the tasks in both chapters are the responsibility of the safety authority (not the ministry). And "7.3.3" and "7.3.4" have to be changed to "5.3.3.3" and "5.3.3.4". See bullet points 4 and 5 in comment 5.
22	Report 2.5.1: Figure n°1D	40	In chapter 5.3.3.1 is explained that the safety acceptance seekers are only the RU and the IM. Chapter 5.3.3 says, that this process is running on level 4. This is right. But is has consequences in figure 1D: • On the left side in the upper box the word "supplier" has to be deleted. • In the diagram the question "Is it a supplier" has to be deleted. And the whole YES branch of this question has to be deleted, too. At the top there are three boxes with the inserted text parts "(7.2.1)" and "(7.2.2)" and "(7.2.3)". These have to be changed to "(5.3.3.1)" and "(5.3.3.2)" and "(5.3.3.3)". At the left side there is a box with the inserted text "Notified Organisation). See comment 7.
23	Report 2.5.1: 5.4 Example	41	Regarding the figure and as mentioned above: In the row "(RU, IM)" are the two boxes "Signalling system approval" and "SMS approval". But in the Safety Directive IMs and RUs are no approving entities. So it is required to find other names. See bullet point 3 in comment 5. If the Member State has installed a Safety Authority it is the task of this body authorising the bringing into service. So the last line should be deleted. See bullet points 4 and 5 in comment 5.
24	Report 2.5.1: 6.1. Purpose	42	This paragraph says: *"[…]. Especially for the cross-acceptance-process which should guarantee interoperability it is important to have a common assessment-method."* The sentence seems to imply that interoperability is mainly achieved by cross-acceptance. This is rather misleading be-

			cause interoperability can also be achieved through other means (e.g. standards). However, cross-acceptance is a very important matter in order to reduce the costs to launch new systems and components in railway networks.
25	Report 2.5.1: 6.4 Specifying the Requirement of the Assessment	45	This paragraph says: *"The requirement of the assessment will be produced by the assessor in close consultation with the client. The final version of the Assessment Requirements Specification must be authorised by the client."* In this paragraph the word "client" is used two times. This word is not precise enough. We think it should be used "the body using the content of the assessment report".
26	Report 2.5.1: 6.6 Assessing Products and Operational Processes, paragraph 4.	48	This paragraph says: *"The main activities of product assessment are to ensure that the safety requirements are complete and consistent with the safety requirements, and that the safety integrity requirements for those functions are correctly assigned. […]:"* What does the first part of the sentence mean? The content cannot be understood.
27	Report 2.5.1: 6.6 Assessing Products and Operational Processes, paragraph 5.	49	There are 7 bullet points. Hereafter: It should be mentioned, that the assessment work can be based on the verification and validation work.
28	Report 2.5.1: 6.8.3 Independence and Neutrality	60	The second paragraph says: *In EN 50129 it is stated that the safety assessor should not belong to the same organisation as the project team, the verifier or the validator. In specific cases the assessor could be part of the same organisation as some of this parties, but other measures must than be taken to assure safety. One possible solution is a direct line of reporting between the assessor and the safety authority.* Germany (the EBA) has gained very good experiences with this regulation. It should be verified whether this solution can be expanded.
29	Report 2.5.1: 6.8.3 Independence and Neutrality	60 - 61	There are two tables defining the independence of assessors. This proposal comes from the "Yellow Book" (UK). This part of the chapter can not be accepted because it is not in line with the experience in Germany and in other countries. There is no reason to make differences between "independent person", "independent department" and "independent organisation". In some cases there are better experiences with "independent persons and departments". How independent are "independent person" and "independent organisation" if they depend on purchase orders? It seems that "independence" is overvalued compared with "knowledge". See also EN 45005 and EN 45011 used elsewhere to define inspection and notified bodies, not mentioned in this report.
30	Report 2.5.1: Table, line GC2	68	For technical systems, sub systems and components 3 years is a very short time. It should be considered to define a much longer time. Such a short time will rise the required effort and will drive the costs.
31	Report 2.5.1: Table, line GC7	68	Only module B is mentioned. It should be considered whether the other modules (as in the TSIs) can be applied. Why should we have a distinction between the TSI and the field not covered by the TSI.
32	Report 2.5.1: 7.2.5 Analysis of a generic example	70 - 75	A clear distinction should be made between: • Constituents and subsystems covered by the Directives 96/48/EC and 01/16/EC;

	example		• Other safety relevant technical components and systems. This is important because in the first case an interoperable asset has to be certified. In the second case the certified asset has not be interoperable. In this chapter we speak about TSI Cross acceptance: *[….]. This validation has to follow a process based on 96/48 [E1] decision and TSI [E3], as it is an interoperable product (7.2.5.1, paragraph 1).* As there is no indication we think that the product is a constituent in the sense of the Directives and TSIs. Therefore it is confusing to read in chapter 7.2.5.2, what has to be done in an acceptance process regarding an interoperable and certified constituent. Could it be that this example is not in line with the Directives and TSIs? There should be two chapters with a clear distinction: • Constituents and subsystems covered by the Directives 96/48/EC and 01/16/EC (and the regarding TSIs); • Other safety relevant technical components and systems (like interlockings, level crossings etc.). We propose to check the content in this example and to add another example regarding the second bullet point.
33	Report 2.5.1: 7.2.5.1 Initial validation	70	The first paragraph says: *"In a first step, the product has to be validated. This validation has to follow a process based on 96/48 [E1] decision and TSI [E3], as it is an interoperable product."* The Directive 2001/16/EC and the TSI for conventional lines should be mentioned, too.
34	Report 2.5.1: 7.3.2 Proposal	79	*"The proposal relates to the case of a product already certified and which corresponds to the triangle of the Safety Case extension due to non-compliances (c.f figure n°1)."* There should be two chapters with a clear distinction: • Constituents and subsystems covered by the Directives 96/48/EC and 01/16/EC (and the regarding TSIs); • Other safety relevant technical components and systems (like interlockings, level crossings etc.).
35	Report 2.5.1: 7.3.2.2 Actors, roles	79	See comment 5.
36	Report 2.5.2: 5.1 ALARP and safety targets and 5.2 General probabilistic acceptance criterion and 5.3 General probabilistic acceptance criterion and 5.4 Acceptance Criterion No. 1: Wrong side failures	16 - 22	The whole report (but especially these chapters) is presenting the UK viewpoint. It is not always in line with the viewpoints in other Member States. Another problem is that only the signalling sector but not the whole railway system is considered. Are the proposals also valid for rolling stock, energy and civil construction? This is a question without an answer. But it is important to create a solution valid for all parts of the railway system.
37	Report 2.5.2: 5.2 General probabilistic acceptance criterion	17	Some statements in this section are misleading. It should be clearly mentioned that the SIL tables allow only one direction of interpretation. First, the THR has to be determined (e.g. 10^{-9}/h) and then the SIL can be derived. It is wrong to do it vice versa. To develop a system according to SIL 4 does not mean that a failure rate of 10^{-9}/h will not be exceeded. SIL 4 only makes

			sure that systematic failures are reduced. In order to ensure that a certain failure rate is achieved, an analysis of the random failures has to be undertaken (usually a fault tree analysis).
38	Report 2.5.2: 5.2 General probabilistic acceptance criterion and 5.3 General probabilistic acceptance criterion	18	It seems that the proposals in these two chapters are not fully in line with the EN 50129. But on the other hand some arguments are true and should be considered. Especially the combination of quantitative and qualitative contributions are very interesting and should be elaborated later on in more detail. So the proposals of the report could be used as a change request for the EN 50129 or launched in the regarded application guide.
39	Report 2.5.2: 5.4.1 Qualitative part – S1	18	Very often the safety level of a part of a system or a whole system is not (precisely enough) known. In these cases the safety target has to be determined by an analysis.
40	Report 2.5.2: 5.4.3 The meaning of wrong side failure	19	The first paragraph includes the following sentence: *"This is illustrated by Table 2, which is taken from HM Railway Inspectorate's Annual Report for 2000/2001 (ref 3)"* It seems it is Table 1.
41	Report 2.5.2: 5.4.3 The meaning of wrong side failure	18 - 20	The content of Table 1 and the following explanations is a short description of the current situation in UK. We can not transfer it to other Member States. So it can not be the basis of a new European solution.
42	Report 2.5.2: 5.4.7 Discussion	21 - 22	It becomes very clear that the proposal and the discussion is specific for the condition in the railway in UK. So it has to be discussed, which parts can be adopted and developed to European rules. So here we can only give an advice like comment 38.
43	Report 2.5.2: 7 Conclusion	27	The paragraphs 1 - 4 could be a kind of overall aim for the work to be done regarding comment 38.
44	Appendix A: Interpretation of ALARP	29 - 32	This part of the report describes how ALARP works in the UK. It is no proposal but only a report on a specific situation. Therefore, we do not see a need to comment on it.
45	Report 2.5.3: 1. Introduction	4	The first paragraph says: *"[…]. The certification demands a process performed by an external entity to the organization that owns the asset being studied."* The word "external" should be deleted. It does not consider the possibilities given in EN 50128 (chapter 6.2.10) and EN 50129 (chapter 5.3.9).
46	Report 2.5.3: 2.2. Definitions	5	The third bullet point says: *Safety approval: Action, without legal consequences, that consists on verifying that an asset, with all the corresponding safety certificates, complies with the requirements specified by the entity issuing the approval (IM or RU),* The term "(IM or RU)" should be deleted, because in some countries (e.g. Germany) this can be the task of another authority (e.g. the safety authority, EBA).
47	Report 2.5.3: 2.2. Definitions and very often also in the chapters 3 - 8.	5	The seventh bullet point says: *Notified organization: Entity in charge of evaluating the conformity of an asset against the reference norms or standards, and issuing the corresponding certificate,* Notified organisations (Notified Bodies) are required in the regulated field (covered by the European Directives 96/46/EC and 01/16/EC). In the other (not regulated) field it is not required to notify the organisation. But it must be accepted. So we should speak in this report about "Accepted Body", because it has not to be an organisation (persons are also able

			to perform the evaluation work).
48	Report 2.5.3: 3. Background information, paragraph 6	6	A part of a sentence says: *"[…] we shall refer to the regulatory framework proposed by the directives EN 50126, EN 50128 and EN 50129, and applying the regulations […]."*. For EN 50126, EN 50128 and EN 50129 we should not use the word "directive", but the terms "standard" or "European Norm".
49	Report 2.5.3: 7.1.1 Process diagram	13	The first paragraph says: *"The charts (diagrams) included in the following pages are an example, a model, and not necessarily the only possible way to represent the process defined in each case."* This is a very important sentence. But it is not only valid for the diagrams, it is also valid for the proposals (text) in the chapters 7.2 and 7.3. So we will only mention main points and main problems in these chapters. And we have to see, that the solutions have not to be exactly the same in all Member States if the requirements of the Safety Directive are fulfilled.
50	Report 2.5.3: 7.1.2 Actors and roles	13 - 14	See comment 5.
51	Report 2.5.3: 7.1.3 – 7.3	14 - 24	For EN 50126, EN 50128 and EN 50129 we should not use the word "directive", but the terms "standard" or "European Norm".
52	Report 2.5.3: Chapter 7.1.3	14	In this chapter two times the term "independent evaluation" is used. That may be right in some cases. But in the case of technical items the term "assessment" should be used in line with the EN 50126 - 50129.
53	Report 2.5.3: Chapter 7.1.3,	14	The last sentence in paragraph 2 says: *"The justifications or Safety Cases need to be grouped as the integration process takes place such that the last safety case, the Application case, which will refer to the "smaller" cases grouped within it, will allow the safety authority to issue the certificate of acceptance and to defend the putting into service request in front of the ministry of transport."* We think this proposal is not in line with the Safety Directive. See comment 5, third bullet point.
54	Report 2.5.3: 7.1.3 – 7.3	14 - 24	A clear distinction should be made: • Constituents and subsystems covered by the Directives 96/48/EC and 01/16/EC; • Other safety relevant technical components and systems. This is important because in the first case the certification has to be given by a notified body (in line with the two directives) and in the second case the certificate issued or the assessment can be performed by another accepted organisation or person.
55	Report 2.5.3: 7.2.2 Analysis and test and diagram in chapter 7.2.3	16, 18	Paragraph 2 contains the following sentence: *"The notified organization will verify the certification process followed in the elaboration of the certification report."* And the diagram contains specific boxes for this case. Why shall the organization certify the certifications process? This process is driven by the organization. So it should be possible to merge the certification of the asset and the management of the certification process. Then only one report regarding the certification should be issued.
56	Report 2.5.3: 7.2.4 Complaint and certificate suspension	18 - 19	In the last paragraphs of this chapter the following possibility should be described: The seeker will add or change the documentation or the technical solution. After that the certification process will be continued.

57	Report 2.5.3: 7.2.5 Maintenance of the Certificate	20 - 21	In this chapter and in the right part of the diagram in chapter 7.2.4 it seems that in the case of a renewal the whole certification process has to be performed once more. If there is no modification regarding the asset: why the whole process has to be performed? Two sub processes have to be defined: Renewal the certification in the case of a non-modified asset. Renewal the certification in the case of a modified asset. Or is the process described in chapter 7.2.6 the renewal process? This is not clear, because the connector in the right part of the diagram in chapter 7.2.4 leads to the diagram in chapter 7.2.3 with the whole certification process.
58	Report 2.5.3: 7.3 Safety acceptance and authorization for service	22	Paragraph 2 says: *"The certification process performed in this second part completes the global process of certification. The scope of the safety acceptance and authorization for service process converts an asset with its approval certificate to an asset ready for operation. Therefore, the aim of this part is an operational level certification including the certification of rules and procedures, the asset is considered in the context of operation (level 4, see section 4 of this document)."* To avoid misunderstandings we should not speak about a certification process but about an acceptance or better approval process.
59	Report 2.5.3: 7.3.3 Decision and 7.3.4 Authorization for service (opening the line) and diagramm in chapter 7.3.4	24	The last paragraph in chapter 7.3.4 says: *"In the case where the safety authority belongs to the Ministry of transport, the sub-process 7.3.3 and 7.3.4 could be joined and understood as a single activity. In this situation, the safety acceptance and the authorization for the service will be achieved in one step."* That is right. But in the case that there is a safety authority (normal case) the Safety Directive determines that the tasks in both chapters are the responsibility of the safety authority (not the ministry). See bullet points 4 and 5 in comment 5.
60	Report 2.5.3: 8. Example	25	See comments 7 and 23.
61	Report 2.5.4: 1.1. Objectives, 2. paragraph.	3	See comment 24.
62	Report 2.5.4: 3. Specifying the Requirement of the Assessment	6	See comment 25.
63	Report 2.5.4: 5. Assessing Products and Operational Processes, paragraph 4.	9	See comment 26.
64	Report 2.5.4: 5. Assessing Products and Operational Processes, paragraph 5.	9	See comment 27.
65	Report 2.5.4: 7.1. Technical and Individual Knowledge	18	See comment 28.
66	Report 2.5.4: 7.3. Independence and Neutrality	18	See comment 29.

67	Report 2.5.5: 1.1 Objectives	4	The second paragraph says: *The objective of the report is to assess how the common criteria and assessment method defined as per 2.5 relate to AEIF's (French Association for Interoperability) and IMDR-SdF cross-acceptance approach [E5].* The explanation of AEIF is not correct.
68	Report 2.5.5:	all	This report is mainly based on the work and proposals of ERC Committee (ERC - European Rules of Conformity). The aim of ERC (set up by UIC, UITP and UNIFE) is the harmonisation of conformity assessment practices in the voluntary field (the field not covered by the European Directives 96/48/EC and/or 2001/16/EC; regulatory domains). So ERC and its work can create a basis for cross-acceptance. The proposals in this report are likely the same as in the ERC papers: • Guidelines for the Competence in the Railway Field (Parts 1 - 4) and • Guidelines for the Acceptance of Railway Product certification. Acceptance is not the main item of SAMRAIL. But it is important to be discussed. Report 2.5.5 includes a big number of (partly) very detailed proposals. Because report 2.5.1 is understood as a summary of all other reports in this work package, no detailed comments are given here on report 2.5.5. This does not mean that all proposals can be accepted. It seems that the effort for a cross acceptance process based on the proposals in this report is bigger than required.

Work Package 2.6

Nr.	Text source	Page	Comments
1	6.4.1 Situation in some EU countries	28 - 30	In this chapter only the paragraphs regarding Germany have been assessed by the VDB.
2	7.1 Review of basic principles of safety design and operation of the railways (paragraph 1)	31 - 36	The first two sentences say: *"The railway system is designed to be a "fail-safe" system. Each failure susceptible to produce harm shall be: […]"* That is true (fail-safe-system) for main parts of signalling and some parts of rolling stock. But many other parts are not designed as fail-safe system, because it is either not deemed necessary or simply impossible (e.g. rails are not fail-safe!). The two bullet points (on page 21/32) are only applicable on signalling systems. A technical solution of just one supplier is described. But the safety principles used from other suppliers provide the required safety too. We propose to delete such special and partly questionable parts from the report. On page 32 there is the following sentence: *"The great majority of the standards, directives, regulations and guidelines for technical design and safe operation apply the basic consideration shown above."* With a view on power installation, rolling stock, and civil structures this sentence is not true. The sentence *"A system that is perfectly designed [...] is 100% reliable and [...] is also 100% safe."* is wrong. A perfect design would only exclude systematic failures. Random failures, however, cannot be **completely** avoided, no matter how well the design may be, because not all parts of the railway system are fail safe. Combinations of such random failures may eventually lead to hazards and accidents. By implementing redundancies, the probability of hazards caused by random failures can be significantly reduced but not fully excluded. We propose to delete this sentence because it is not required and it is misleading. In the second paragraph on page 34 there is the following sentence: *"The persistence of failures category 2 and the operation in degraded mode provide a higher risk that barriers are penetrated and the system passes into the unsafe region."* *This sentence should be changed as follows: "The persistence of failures category 2 and the operation in degraded mode provide a higher risk."* If it was an unsafe situation it would by law not be allowed to operate in this situation. Therefore this sentence must be changed. In the third paragraph on page 34 there is the following text in brackets: *"(could be residual, systematic failures that were not considered in the fail-safe design)".* The text in brackets should be changed as follows: *"(could be residual, systematic failures that were not considered in the design)"* because this is also true for "non-fail-safe design". The third paragraph on page 14 says: *"The document contains, in italics, some more detailed explanations aiming at supporting the main findings and conclusions. These text may*

			not be included in a final report. We propose to exclude it from the final report. Therefore we will not give comments on the pages 35 and 36. The whole section 7.1 should be reviewed with regard to its applicability to the whole railway system. The current contents seems to focus only on a very small part of safety related railway systems and functions (mainly signalling).
3	9 Structured approach to safety indicators	39	A "safety indicator related to incidents" is proposed. It has to be stated very clearly that only a certain part of incidents will be discovered. For example, it may happen that only a single person discovers a failure or makes a mistake. If this person or a small and closed group of persons is responsible for this situation which is not discovered by others this incident will not be reported. Therefore the "safety indicator related to incidents" will not show the real situation and it is problematic to name this a "safety indicator […]".
4	10.1 Incidents	40 - 42	See also the comment on "9 Structured approach to safety indicators" regarding "not discovered incidents". This problem should be mentioned in this chapter.
5	10.1 Incidents, chapter categories	40 - 41	There are only categories mentioned regarding technical problems. We think it should be also proposed to define categories regarding mistakes of staff (important human factor).
6	10.2 Accidents; categories	42 - 46	We must stress that especially the definitions of accidents are not in line with the explanations in other SAMRAIL reports. It should be possible to summarise the different proposals to only one proposal coming from SAMRAIL (last paragraph on page 43).
7	11.1 Quality of data	47 - 49	See also the comment on "9 Structured approach to safety indicators" regarding "not discovered incidents". This problem should be mentioned in this chapter because it affects the quality of the data.
8	11.1 Quality of data (nota)	48	The first two sentences say: *"In the context of using risk indicators at high high level it is not possible to define indicators with high sensitivity to change. It was discussed in a previous section that indicators with high sensitivity to change can not use only data on accidents, but shall implement more technologically oriented knowledge to predict (observe) the potential effects."* This explanation is shared by us. But there is a very important problem. In this report it is mentioned several times that data on accidents and incidents have to be collected. But it is not clearly enough said that it has to be made the following distinction: 1. For safety indicators (and safety targets) only data on accidents (not incidents) can be collected. For CSI (and risk indicators as called sometimes in this report) in other work packages we have the definition: "probability of harm * severity of that harm." Because incidents do not produce harm the data on incidents can not be a contribution to the data regarding risks. 2. Another case is it to investigate the results of changes in safety rules and operational rules or of the introduction of a new system or a new technology. Here the data collected from accidents and incidents can be applied to get more sensitive results and to make statements much more earlier. Therefore a very clear distinction has to be made between CSIs and / or risk indicators and indicators regarding acci-

			dents plus incidents (a name has yet to be given).
9	12. Organisational Learning from Accidents and Incidents in European Railways	54 - 86	In chapter 11 is not mentioned that the manufacturer (or supplier) of rolling stock and safety related infrastructure components can have an access on the data base. But this is a very important possibility for the manufacturer (or supplier) to set up an own learning process. Therefore in chapters 12 should be mentioned that the manufacturer (or supplier) can also have a (eventually restricted) access on the collected data. This is a very important contribution to increase the safety of rolling stock, civil structures, and technical installations. Very important in this respect are data on technical reliability. This way the manufacturer (or supplier) can contribute to the learning process of RUs and IMs. An example is given on page 67.
10	13 General conclusion (second sentence)	87	The sentence says: *"Distinction should be made between the indicators with high sensitivity to changes that shall be used in the multi-loop & feed-back structures of a SMS and the synthetic high level safety indicators for monitoring the safety and the results of safety policy."* We think this is the right way and it is very important. This problem should be intensively explained in a separate chapter in the report (see our comment on "11.1 Quality of data (nota)").
11	14.3.1 Equivalent fatality	93	The table entry for Germany should be changed because the formula (originating from the publication of MEM) is not considered in official certification procedures in Germany. Suggestion: *"10 serious injuries or 100 minor injuries (used in application of the MEM principle but not officially stipulated)"*

Work Package 2.7

Nr.	Text source	Page	Comments
1	Report Document Abstract	2	This paragraphs says: *"[…]. Also many particular, practical questions of safety assessment and use of standards for safety issues that have not been discussed in the directive will be solved within this work package. Since the approach developed here is based on best practice, i.e. experience of persons and organisations already working for a long time in the field, the results are directly applicable for all those working in safety assessment or system development. […]"* We can not agree with this statement. The report actually does not fulfil this proclamation. In the following part of this table there are many remarks on problems in this report. These problems have to be solved before claiming that the described methods are really the 'best' practice.
2	Report 1 Introduction, paragraphs 4 - 6	7	These paragraphs say: *"The report is based on different sources. Many sources have been indicated explicitly. In addition, material has been used that appear for the first time in this form. These parts are based on the author's own experience in many projects.* *[…] In this report, most of the methods described as best practice have been experienced by the authors. The methods have proved to be effective and productive.* We have to see very clearly that this report can only be based on a part of all gathered experiences. So we have to see that there can be more and other good solutions; perhaps with better results in practice.
3	Report 3.1 Existing Gaps in Standards, paragraph 4	10	This paragraph says: "*The definition of safety integrity levels and the requirements to the design, design processetc. are only explicitly defined for control and signalling, see EN 50128 [23], EN 50129 [24]. A safety integrity level consists of two main requirements. The first one is that the function of the object in regard shall not exceed a target value for dangerous failures. Second, certain design requirements have to be fulfilled. EN 50129 presents design requirements for signalling and control. Currently it is not clear, how these requirements can be adopted for other electrical and electronic subsystems or even mechanic or pneumatic subsystems."* This paragraph includes a very important statement and it is true. There is no balance between signalling, rolling stock, electrical installations and civil structures. Today often quantitative hazard analyses are carried out for signalling issues. But this is seldom done in the area of rolling stock and electrical installations. It may depend on the fact that in the latter area are no standards defining SILs and the consequences of definied SILs (like EN 50129 und EN 50128). Regarding civil constructions (and mechanical system in general) this is totally unusual. There are only standards how building and infrastructure have to be constructed to be safe enough. This leads to an unbalanced situation. Safety targets shall be valid for the whole railway system and then be apportioned to specific subsystems. But does it make sense to apportion these targets to subsystems when in a wide range of the rail-

			way systems no standards exist to transfer these targets in practical technical solutions? It seems to be that there are no experiences on which these standards could be based. If it is unknown, how to construct a civil building to fulfil a specific quantitative safety target, than it is also not possible to make an economic apportionment of safety targets for the railway system. In this case we do not know whether the safety targets of the subsystems can be fulfilled in an economic way.
4	Report 5.4 Efficiency of Safety Concepts in Different Areas, last paragraph	48	There it is said: *"When using methods from section 5 in the railway one needs to bear in mind that the usual expenses for safety in railway are usually smaller than in those areas. Therefore, the methods need tailoring to apply them."* These two sentences are a kind of conclusion. But no proof for the truth is given. The cost for safety assessment and demonstration are clearly smaller but not necessarily the cost for safety.
5	Report 5.2.1 2) Severity must also include other damages, besides those to persons, paragraph 1 and 2	50	The following paragraphs are right: "*Accident severity must take into account* – *damage to passengers, personnel, third parties,* – *damage to material values (goods as e.g. payloads, equipment, third party's belongings),* – *damage to environment,* *see [25] as an example.* *Here, material losses or environmental damage have to be included. In these cases, the damage can be measured in monetary units, although this might be complicated in some specific cases."* Damage to material values and to the environment belong without doubt to the results of accidents. These items should be included in accident reports. But it results in much work to include these consequences in risk and hazard analysis and makes these analyses more expensive. We prefer the proposals in other SAMRAIL reports that only take damage to passengers into account.
6	Report 6.2.2 Discussion of the MEM, GAME and ALARP Principal, last paragraph	51	This paragraph describes the risk graph method from IEC 61508. In our opinion, this method should not be mentioned in the same context as MEM, GAME and ALARP. The reason is that the risk graph (in contrast to the other principles) is **not** based on quantitative risk analyses.
7	Report 6.3 Overview on Tolerable Risk Values and Existing Risks	52 - 61	It is very disappointing that this section does not provide the EU transport risk statistics for comparison. Such statistics are available to the public via the internet at no cost! When writing about "Existing Risks" a look at these statistics should be self-evident.
8	Report 6.3.1.1 Kuhlmann's Approach	52	In order to avoid misunderstandings, this section should also mention the more commonly used name of "Kuhlmann's Approach": the MEM principle.
9	Report 6.3.1.4 Safety Integrity Levels in Different Standards, paragraph 2 (and in other positions in the report)	58	This subsection does not fit into the section 6.3.1 on "Existing tolerable risk values and achieved risk values". Safety integrity levels are related to hazard rates of functions and systems but **not** to risk. (Whether a system has SIL 4 or SIL1 allows no immediate conclusion about the risk associated with the system!). The first sentence of this paragraph says: "*It must be noted furthermore that the data given in the three standards EN 50129 [24], IEC 61508 [33] and DEF-STAN 00-56 [10] are tolerable rates of dangerous failures of technical*

			systems, whereas the other rates (maximal tolerable risk values) discussed so far are rates describing the occurrence of accidents." This sentence is speaking about tolerable rates and values. We have to point out that the mentioned standards do not define **tolerable** rates and values. Tolerable rates and values are results from a derivation of the safety targets and risk analyses, but not from these standards. The standards "only" tell you what to do for demonstrating that a system complies with a given tolerable hazard rate. The standards do **not** provide risk targets and they do **not** provide tolerable hazard rates!
10	Report 6.4 Proposals of Safety Targets in Terms of Terms of Risk	61 - 66	The author of the report lays too much emphasis on the MEM principle. In the railway sector this principle is not dominating the process of setting risk targets. It is only used as an additional principle to assess the results coming from other processes. Today GAME and ALARP are the mostly used principles. In some countries the GAME principle is the basis of the legislation. And also the new Safety Directive is largely based on this principle - without mentioning it explicitly. We propose to revise the chapter of the report and to develop a new strategy for setting risk targets. This strategy should be in line with the essential idea of the new Safety Directive.
11	Report 6.4.2 Example	62 - 66	The whole section 6.4.2 is poorly described and misses information that is necessary to understand the calculations. Table 6.4.2-1 is not adequately explained. The meaning of the values is not given, e.g. what does *"average number of fatalities in the class"* mean? The text says *"It shall be noted that the value of 1.02 10^{-2} obtained from Kuhlmann's heuristic approach is about 5 times smaller than the value for realistic transport systems as e.g. metro systems."* What is the mentioned value? What is its unit (fatalities, dimension-less probability)? Where does the statement concerning a metro system come from. The calculation of the ALARP boundaries is not sufficiently justified. Additionally, we miss the influence of the dimension (km of lines, density of the traffic, etc.) of the railway system. Or has Kuhlmann explained it for only one accident? We propose to delete the chapter 6.4.2 because it seems to be inadequate.
12	Report 6 Overview of existing safety compliance criteria and proposal of a harmonised set of criteria based on best practice.	49 - 77	There is not much "overview" in this section. Instead, the text concentrates very much on the authors' proposal. Furthermore, we doubt that this proposal is actually best practice. In some respect it even is in contradiction with the EU Safety Directive.
13	Report 6.5.1 Risk Apportionment for New Systems	68	The text says: *"For each hazard, an expert estimate of severity and occurrence frequency is given."* This statement is very misleading because hazards do not have a severity. Accidents have a severity and sometimes a hazard may lead to an accident. The difference between hazards and accidents must not be neglected. Otherwise the risk analysis will not lead to useful results. The text claims *"Experience shows that railway safety authori-*

			ties give risk requirements […] in the form of an ALARP region". This statement is wrong! In fact, only the safety authorities in a very few countries provide quantitative risk requirements at all. Requirements in terms of an ALARP region are a seldom exception. The sentence has to be changed.
14	Report 6.5.1 Risk Apportionment for New Systems, paragraph 3	68	This paragraph says: *"To be consistent with EN 50129 [24], the approach of risk apportionment has to be carried out in the following steps. Risk apportionment is done first for the system functions and then the risk budget is further broken down. That means, the procedure described above has to be repeated several times. […]"* And the EN 50129 says ("Scope"): *"This standard is applicable to safety-related electronic systems (including sub-systems and equipment) for railway signalling applications."* "*Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)."* We have to see that the described procedure - as that is based on standard EN 50129 - can be relevant for signalling applications. But it may be very difficult or not possible to apply it to rolling stock, electrical installations, and especially civil structures. The present version of the report does not propose procedures for non-signalling applications. But that is the bigger part of the whole railway system.
15	Report 6.5.1 Risk Apportionment for New Systems, number 2., paragraph 2	69	There is the following text: "*In this step, risk apportionment is first carried out for the system level safety functions. In accordance with EN 50129 [24] the definition of safety integrity levels can be carried out only for system level safety functions. Further apportionment is applicable to risk values, but not to Safety Integrity Levels. Assignment of Safety Integrity Levels is carried out using the obtained risk budget for the coinciding function and obtaining from the risk budget a permissible value for the rate of technical failures for the safety related function. From the latter, the Safety Integrity Level can be derived consulting the Tables 6.3.1-5 or 6.3.1-6 according to the applicable standard."* As the definition of safety integrity levels is in accordance with the standard EN 50129 only table 6.3.1-5 should be used. The description of the EN 50129 process is not fully correct: • The statement "Further apportionment is applicable to risk values" is not appropriate, because there are no risk values on this system level, only hazard rates or failure rates. • With regard to the correct system level for SIL allocation, EN 50129 is not as clear as the SAMRAIL text proposes. EN 50129 talks about "system functions" at a "functional level" and not about "system level safety functions". Other CENELEC sources state that the SIL allocation has to take place just at that system level at which the systems involved are still functionally independent.
16	Report 6.5.1 Risk Apportionment for New Systems, number 2., paragraph 2	70	The text says *"[…] however it must be demonstrated by adequate techniques as e.g. Failure Modes, Effects and Criticality Analysis (FMECA) or Fault Tree Analysis (FTA) that the unit has a rate of dangerous failures not exceeding […]".* FMECA is **not** an adequate technique for quantitative analyses and should be deleted from the text.

17	Report 6.5.2 Risk Apportionment for Existing Systems, paragraph 1	71	The first sentence is: "*In most of the cases of existing railway related engineering work, an existing railway system is altered or extended.*" We fully agree with this sentence and like to underline it. In the practice in the railway sector there are no new systems in the sense of chapter 6.5.1. Also constructing a new line is an extension, as mentioned under 1) in the next paragraph.
18	Report 6.5.2 Risk Apportionment for Existing Systems, number 1)	71	In the case of extensions we see another process. On the basis of the new Safety Directive safety targets have to be defined. In other SAMRAIL reports proposals are made for the dimension of the safety targets (e.g. fatalities / person kilometre or fatalities / train kilometre). If we have an extension of a railway network the new part of the railway system has to reach the specified safety targets for this part.
19	Report 6.5.2 Risk Apportionment for Existing Systems, number 2a)	72	This can only be a basis. For the future it is not sufficient because the new Safety Directive requires safety targets to be considered.
20	Report 6.5.2 Risk Apportionment for Existing Systems, number 2b), last two paragraphs	73	We think this explanation is not best practice for the future. The results of the analysis are compared with the results derived from the MEM principle. But in the future the results of the analysis have to be compared with the common safety targets. A comparison with the GAME principle under consideration of the common safety targets might be a possible way.
21	Report 6.5.3 Evidence of fulfilment of the Risk Target	75	Our remarks with the numbers 18 - 20 are also valid in this case.
22	Report 6.5.3 Evidence of fulfilment of the Risk Target	75 - 76	FMECA is not a suitable method to calculate failure rates (see also comment above).
23	Report 7 Practise of safety assessment and propose a guideline for safety assessment based on the common compliance criteria.	78 - 122	The assessment scheme proposed in this section is not very cost-effective. It is over-regulated and leaves too little space to adapt for the needs of specific projects. The risk is that too much money will be spent just to fulfil the assessment rules rather than spending money to actually improve safety. We have to be very careful when introducing new extensive assessment requirements because these may eventually lead to a cost increase in European railways. This might be useful for the safety assessors but definitely not for the competitiveness of the railway sector.
24	Report 7.7.2.1 Form and Disposition of the Planning Documents	81	The second sentence says: *"The planning documents have to be achieved together with the documentation of the assessment."* We think a mistake has to be corrected: […] archived […]. Otherwise the sentence makes no sense.
25	Report 7.7.3 Formal Inspection of the Documents of the Assessment Object	82	It seems that the described steps (see annex) are not fully required. Regarding the assessment we have to ensure that only the safety related work has to be done. In this case it seems that there is too much formalism. The European Commission want to revitalize the railway systems. This depends e.g. on the costs of systems. So we have to avoid all things driving the costs without presenting benefits regarding the safety.
26	Report 7.7.4.1 General Require-	83	Regarding the explanation in remark 16: This chapter and the annexes 5 and 6 describe a kind of classification of the manu-

	ments for Manufacturer's Documentation		facturer. But what are the consequences? And who has to do anything? This becomes not clear.
27	Report 7.7.4.2 Goals of the Assessment	83	This paragraph begins: *"During the assessment the following aspects have to be checked:"* Regarding the explanation in remark 16: We can find here a large number of items that are proposed to be checked. It should be considered that the acceptable effort for safety assessment depends on the size of a project. We miss a sentence or a paragraph with a statement that in the case of small and non-complex issues (e.g. simple changes) a large part of the described items is not required. Some examples should explain it clearly.
28	Report 7.7.5.1 General Requirements on Documentation	85	This chapter is not in line with the requirement and derivation of safety targets according to the new Safety Directive. Additionally, measures against systematic failures (following the SIL concept) are only defined for a very small part of the railway system. It is therefore not appropriate to consider the allocation of SIL as a mandatory task.
29	Report 7.7.5.1.1 Method for the Definition of the Tolerable Hazard Rate of the System	85	This chapter is not in line with the requirement and derivation of safety targets according to the new Safety Directive. Additionally: MEM, ALARP and GAME provide risk acceptance criteria and **not** tolerable hazard rates (THR). In order to obtain THR, a risk analysis with subsequent apportionment has to be undertaken.
30	Report 7.7.5.1.2 Preliminary Hazard Analysis	86	The first sentence says: *"Following the definition of the Tolerable Hazard Rate / the Overall Safety Target for the overall system, a first Preliminary Hazard Analysis (PHA) shall be produced immediately at the beginning of the development, as it forms the basis for the Safety Requirements Specification."* As we understand the new Safety Directive, it is the responsibility of the railways to define the safety requirements. The Safety Requirement Specification should be a basis document for the development of a system or subsystem. E.g. it is the task of the railways to define which functions should be implemented in a technical solution and which are the task of the personnel (definition of man-machine-interface).
31	Report 7.7.5.1.3 Allocation of SILs to Functions / Sub-Functions / Systems / Sub-Systems		The remark 30 mostly also valid for this chapter (see realisation by design or functions).
32	Report 7.7.8.2.2 and 7.7.9.2.2 and 7.7.10.2.2 and 7.7.11.2.2 and 7.7.12.2.2 If the V&V Activities are performed under Assessor's Responsibility	96, 99, 102 106 110	There is the following sentence: *"This kind of inspection is not the item of consideration, here. Generally it is necessary in this case, to provide evidence by suitable detailed checks and reports that the criteria mentioned under […] are met."* Additionally, it should be mentioned that such a procedure seems to be not in line with the standards EN 50128 and EN 50129.
33	Report 7.7.12 Operation and Maintenance	107	This chapter deals mostly with the Safety Management System of the railway undertakings and the infrastructure managers. This issue is also the theme of WP 2. It would be a better solution to report on the Safety Management System only in one WP. Now we have partly different proposals. Due to this overlap, we decided to provide comments only on the content

			of WP 2.2.
34	Report 7 Practice of safety assessment and propose a guideline for safety assessment based on the common compliance criteria	78 - 122	This chapter is based on the standards EN 50126 - 50129. The standard EN 50129 (signalling) is a kind of focus. In a wide range it may be possible to apply the described proposals on vehicles and electrical installations, with changes in details. But there are doubts: Is it possible to apply the proposals on parts of the infrastructure like tunnels, bridges, buildings, rails, and points?
35	Report 8 Handling Standards, Rules Regulations And Laws To Build Your Safety Management System	123 - 132	It is not clear which is the regarded Safety Management System. Many chapters are valid for the SMS of the railway undertaking or the infrastructure manager. On the other hand some paragraphs have connections to the development of new items. In these cases not the SMS but the approval procedure is the focus. It should be clearly defined which items have a connection with the SMS and which problems have to be clarified with the railway safety authority and which institution has to clarify it (manufacturer or RU or IM).
36	Annexes	all	It is not deemed necessary to give special comments on the annexes. In some cases the regarding annexes are mentioned in the above comments. In other cases rules from different countries are only listed. It does not seem to be relevant whether the tables are correct or not.

Work Package 2.8

Nr.	Text source	Page	Comments
1	Volume I 2.1 Introduction, paragraph 3 and 2.2 Safety rules: definition and general principles, paragraph 1	11	These paragraphs say: "*The framework was primarily designed to deal with the development and management of operational safety rules and work instructions, e.g. for track maintenance workers, train drivers, traffic controllers, etc. However, during the project it became apparent that the same structure could be usefully applied at other levels of rule management, from the development of law and regulations in ministries and national railway bodies, down through the rail organisations (infrastructure managers, train operators, contractors, etc.) to the operational process. This section of the report will describe the framework and its use at various levels in the railway system. […]. Confusions are possible over the use of words such as "rules", "procedures", "regulations", "work instructions" and their equivalents in all European languages. We use the words 'safety rules' in this report in a very general way to cover many manifestations, all of which have in common that they are:[…]. "* In these two paragraphs the standards or norms (IEC, EN, DIN etc.) are not mentioned. We emphasise that this is the right way, because for development, acceptance and introduction of these standards there are special regulations.
2	2.3.2.1 Define processes, accident scenarios and controls for the activity, paragraph 1 and 2.3.2.2 Choice of controls where rules are necessary, paragraph 1	20 - 21	These paragraphs say: *"Risk analysis is the keyword for the functions in this box, which are fundamental to rule generation. Such an analysis requires a sufficiently detailed description of the processes to be analysed, which, in the case of railway processes, can be divided into description of the parts of the process within each of the organisations involved and description of the interactions between organisations. The processes must be modelled – indicating the crucial system transitions (e.g. from normal running to emergency mode, from operational mode to maintenance and back), the functions to be carried out and the system actors who conduct them. […]In this step it has to be decided how the desired states or behaviour will be achieved. The desired behaviour can be imposed on the system actors in one of the following ways:* *- Technical forcing functions,* *- Administrative standardisation in the form of defined and imposed rules,* *- Self-control through expertise and competence based on practice and acquired knowledge, and* *- social group regulation. […].* We think the following point is not clear enough: It should be very clearly expressed that in this context a decision has to be made whether a process has to be carried out by a technical system or component or by railway staff. If a technical solution is preferred, the process must be described in Functional Requirement Specifications. If a function is carried out by staff, the process must be described in rules. The whole solution (technical and non-technical part of the process) has to be covered by a risk analysis.
3	2.3.2.5 Communicate and train rules, paragraphs 2		These paragraphs say: *"[…]. It would be quite simple and straightforward were it not for the geographically distributed*

	and 4		*processes (particularly for train crews and maintenance workers) and the fact that some parts of the work are contracted out to private organisations, with whom communication operates via contracts and often intermittent communication channels. […].* *An important issue in achieving rule compliance is that those who carry out the rules should know why they are necessary. This information may not be in the rules themselves, and so may need to be imparted during the communication and training phase.* It is spoken about "contracted organisations". It is very important to include the suppliers. This should be separately mentioned.
4	5.1 Define processes, scenarios and controls. Choice of controls, where rules are necessary (box 1 & 2), all paragraphs	36 - 37	The distinction in technical solution and managing by staff is not mentioned. See our comment Nr. 2.
5	5.4 Communicate and train rules (box 5), paragraph 4	44	There are the sentences*: "In general, when new rules come out, the infrastructure manager informs the relevant sections and the contractors about this. Each contractor in turn informs his staff".* See our comment Nr. 3.
6	7 Conclusions	58 - 60	The comments Nr. 1 - 7 are also valid for the relevant paragraphs in this chapter.
7	1. Define processes, scenarios and risk control measures for the activity (paragraphs B – E) and 2. Choose which risk controls need rules (paragraph B) and 10. Modify & improve rules (paragraph A)	65	See our comment Nr. 2 and 5.
8	Volume II	all	In volume II the results of case studies in DK, GB, NL and S are presented. It is not required to give comments on these studies. The results of these studies are part of the content of the report "Regulations, roles of rules and their unification - Volume I".