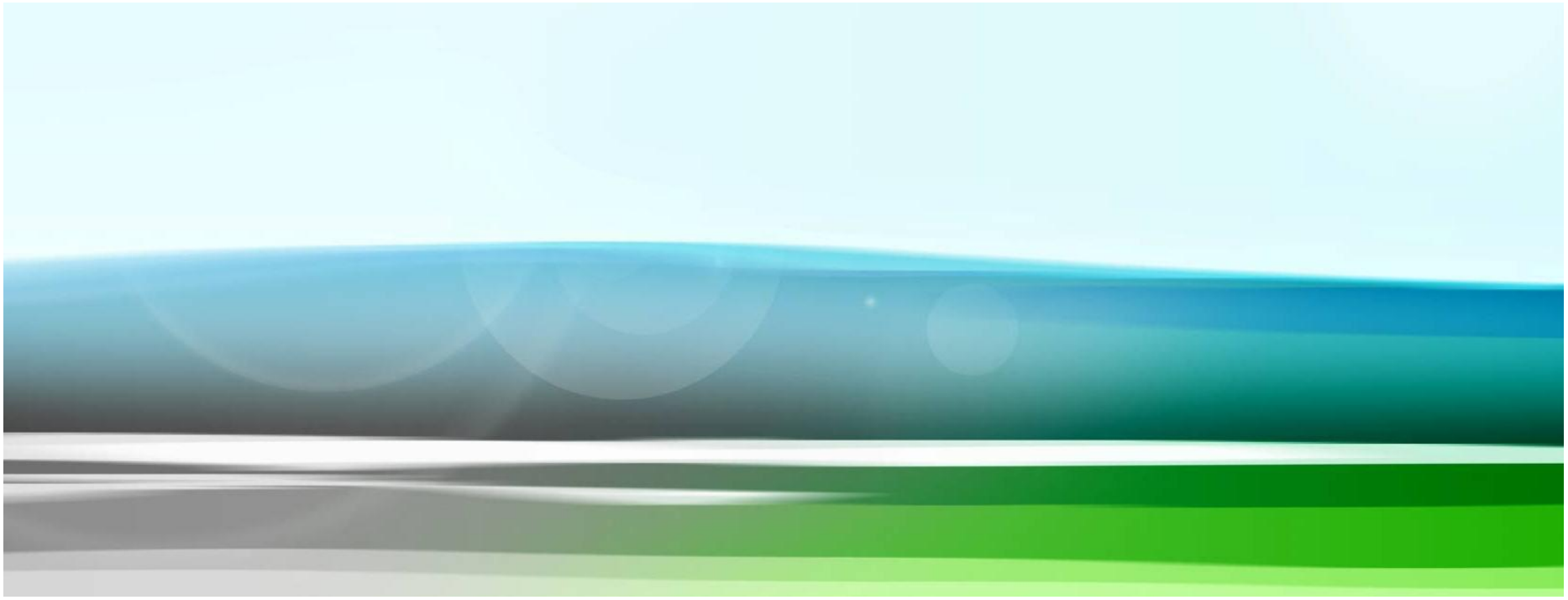


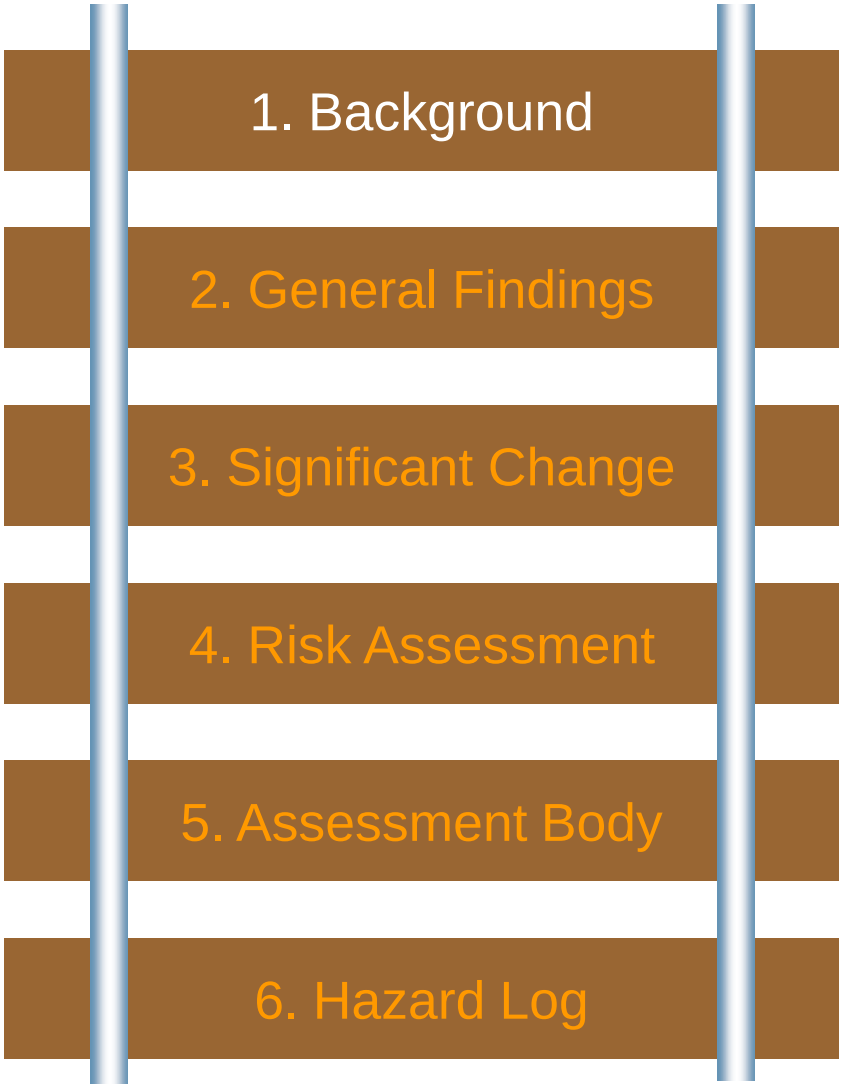
Application of CSM 352/2009 In Europe

Challenges and Results

Gavin Astin
27 Nov 2012

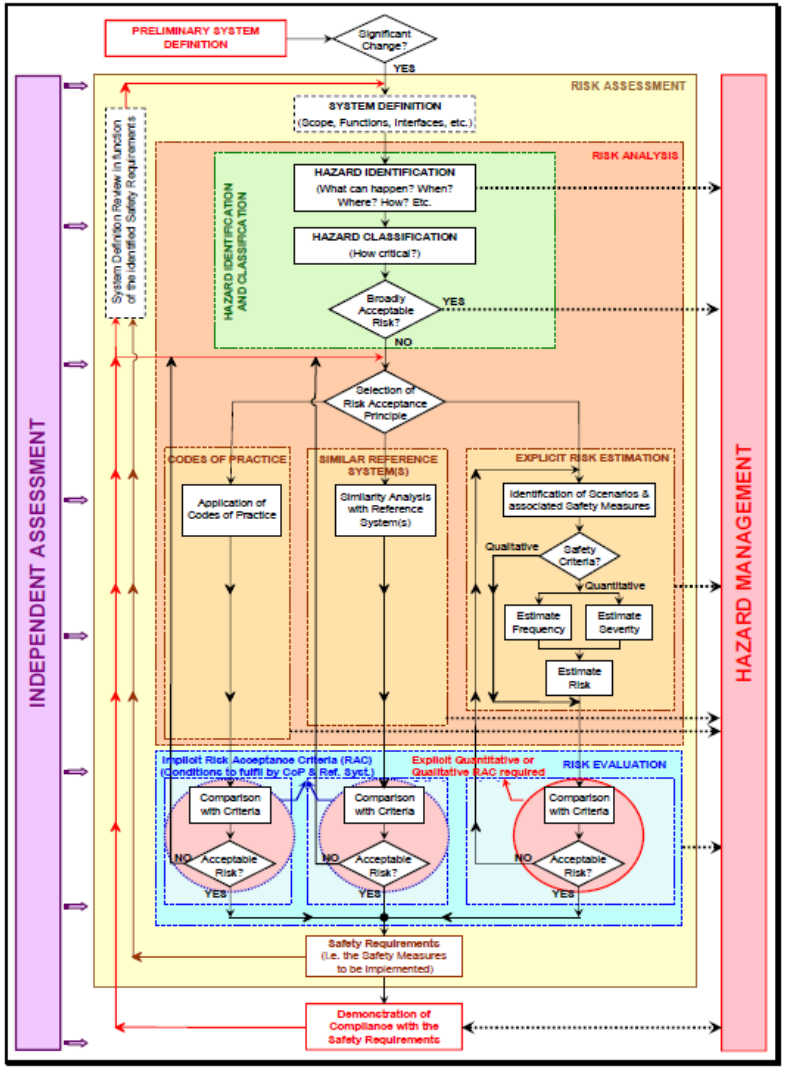
MANAGING RISK DNV

Agenda



Collection of Examples

- There was a previous project with theoretical training material, and our project will support this with practical examples. Not a DNV project.
- Project scope:
  - Contact actors to establish those that have applied CSM RA.
  - Identify those that are willing to share information with the wider railway community.
- Interview actors to establish learning points for each part of the CSM.
- Collate examples and develop a “search tool” for publication (in English).



General observations

- Applied more extensively in countries where risk management is already embedded in an organisation's culture and SMS:
  - In these cases easier to use existing systems and processes to meet the requirements of the CSM RR.
- Little experience of application in Eastern Europe based on our requests for interviews:
  - Because the railway is "stable".
  - Lack of clarity of what makes a change significant.
  - Too early.

Our Database

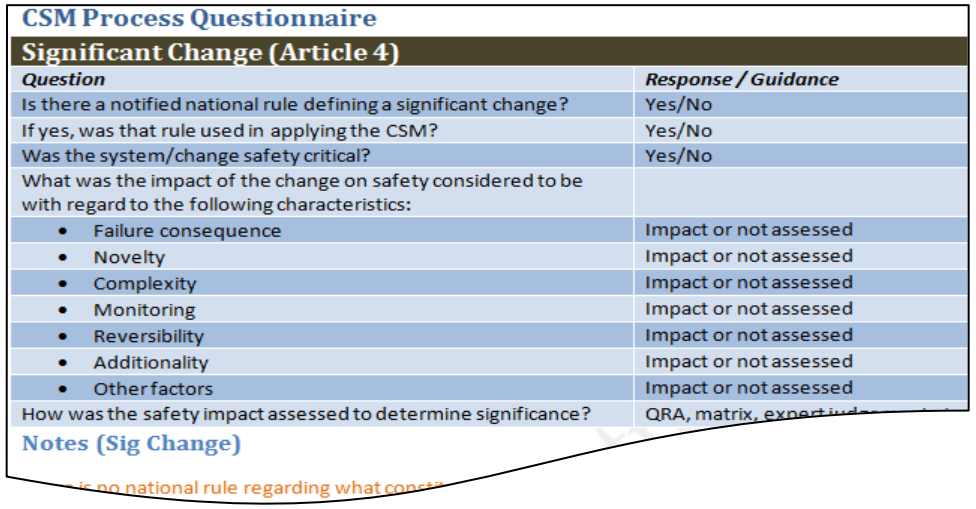
		To start of Example		Significant Change - TM2 Significance of Change	System Definition - TM2 Risk Management on a Project	Hazard Identification - TM3 Hazard Identification, TB RA Techniques	Hazard Classification and Risk Broad Acceptability - TM3 Risk Classification, TB RA Techniques	Selection of the Risk Acceptance Principle - TM4, TM6 Risk Evaluation	Risk Acceptance Principle: Codes of Practice -TM4 Codes of Practice, TM6	Risk Acceptance Principles: Reference Systems -TM4 Reference Systems, TM6	Risk Acceptance Principles: Explicit Risk Estimation -TM4 Explicit Risk Estimation, TM6, TB RAE Techniques	Demonstration of Compliance and Approval of Change - TM7, TM2 Project Safety Documentation, TM5 Mitigating the hazards, TM6	Hazard Management - TM5, TM2 Risk Management on a Project and Project Safety Documentation	Choice of Assessment Body - TM8	Independent Assessment - TM8
Maintenance	T														
	Op														
	Org														
Infrastructure	T	IM_E2		IM_E2	IM_E2	IM_E2	IM_E2	IM_E2			IM_E2	IM_E2	IM_E2		
	Op														
	Org														
Energy	T														
	Op														
	Org														
Locomotive and Rolling Stock	T	RU_E1-SM RU_E3 RU_E4		RU_E1-SM RU_E3 RU_E4	RU_E1-SM RU_E3 RU_E4	RU_E1-SM RU_E3 RU_E4	RU_E1-SM RU_E3 RU_E4	RU_E3 RU_E4	RU_E3 RU_E4	RU_E3		RU_E4	RU_E3 RU_E4	RU_E3 RU_E4	RU_E3 RU_E4
	Op	RU_E1-O RU_E2		RU_E1-O RU_E2	RU_E1-O RU_E2	RU_E1-O RU_E2	RU_E1-O	RU_E1-O	RU_E1-O RU_E2	RU_E1-O RU_E2		RU_E1-O	RU_E1-O	RU_E1-O	RU_E1-O
	Org														
Freight	T														
	Op	FT/ET									FT/ET				
	Org														
Operations and Traffic Control	T														
	Op	IM_E1		IM_E1	IM_E1	IM_E1	IM_E1	IM_E1	IM_E1	IM_E1	IM_E1	IM_E1	IM_E1	IM_E1	IM_E1
	Org	RU_E5		RU_E5	RU_E5	RU_E5	RU_E5	RU_E5		RU_E5					
Control, Command and Signalling	T	IM_P1		IM_P1	IM_P1	IM_P1	IM_P1					IM_P1	IM_P1		
	Op	IM_P1		IM_P1	IM_P1	IM_P1	IM_P1					IM_P1	IM_P1		
	Org														
Process	All	RU_P1 IM_P2		RU_P1 IM_P2	RU_P1 IM_P2	RU_P1 IM_P2	RU_P1	RU_P1 IM_P2	IM_P2	IM_P2	IM_P2	RU_P1 IM_P2	RU_P1 IM_P2	RU_P1 IM_P2	RU_P1 IM_P2

Training modules exist for these

And these are what we have collected

Data Collection Process

- Face-to-face interviews with actors.
- Template for data collection.
- Examples provided were:
  - Specific examples of an application to a particular change.
  - Generic process that could be applied to any change.



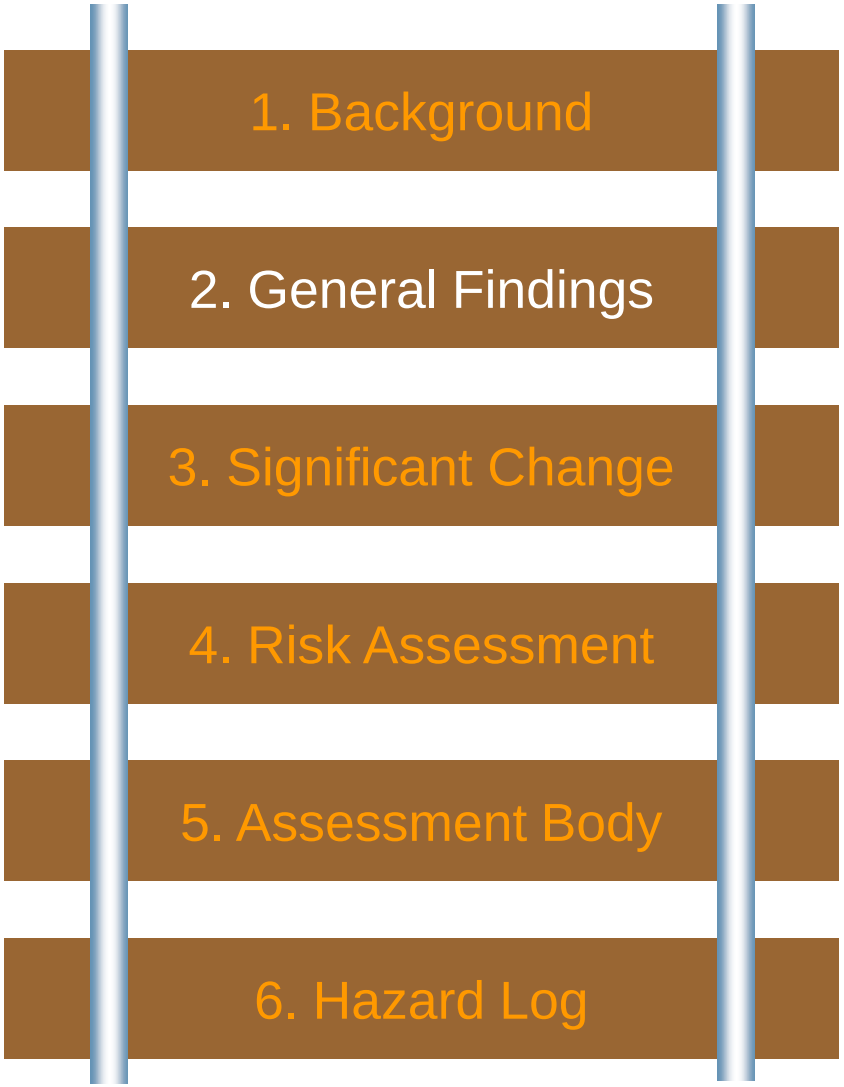
CSM Process Questionnaire

Significant Change (Article 4)

Question	*Response / Guidance*
Is there a notified national rule defining a significant change?	Yes/No
If yes, was that rule used in applying the CSM?	Yes/No
Was the system/change safety critical?	Yes/No
What was the impact of the change on safety considered to be with regard to the following characteristics:	
• Failure consequence	Impact or not assessed
• Novelty	Impact or not assessed
• Complexity	Impact or not assessed
• Monitoring	Impact or not assessed
• Reversibility	Impact or not assessed
• Additionality	Impact or not assessed
• Other factors	Impact or not assessed
How was the safety impact assessed to determine significance?	QRA, matrix, expert

Notes (Sig Change)

is no national rule regarding what const

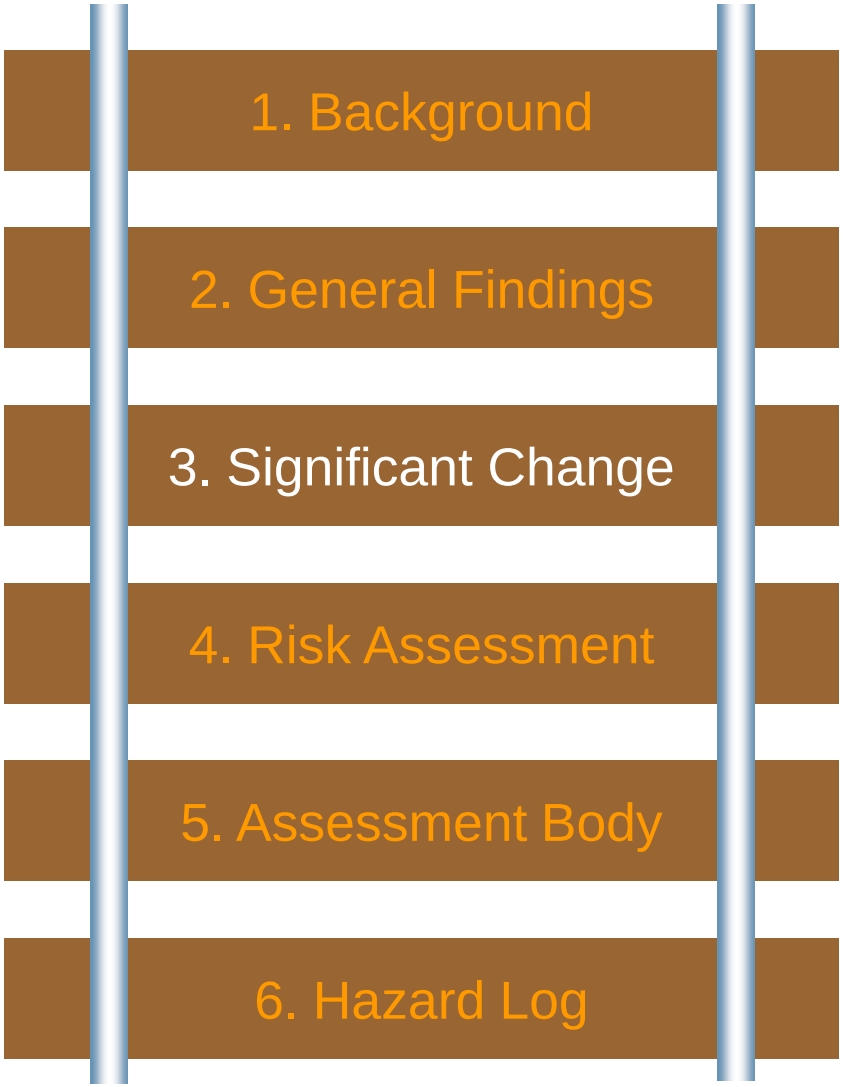


Some general comments…

- The application of the CSM RA is costly and time consuming. It is likely to result is additional information being generated and requiring review, validation, update, storage etc.
- Some cross border differences in understanding of the CSM RA have already come to light. For example, the concept of change significance is not understood similarly between the actor's country and a neighbouring one.
- Some actors tend to answer "No" to the change significance question, in order to avoid applying the CSM RA in full.
- CSM RA is too theoretical and doesn't reflect what happens in practice.
- The CSM RA involves the addition of a third actor (assessment body), which means increasing time, costs and "bureaucracy" and possibly duplication of work.

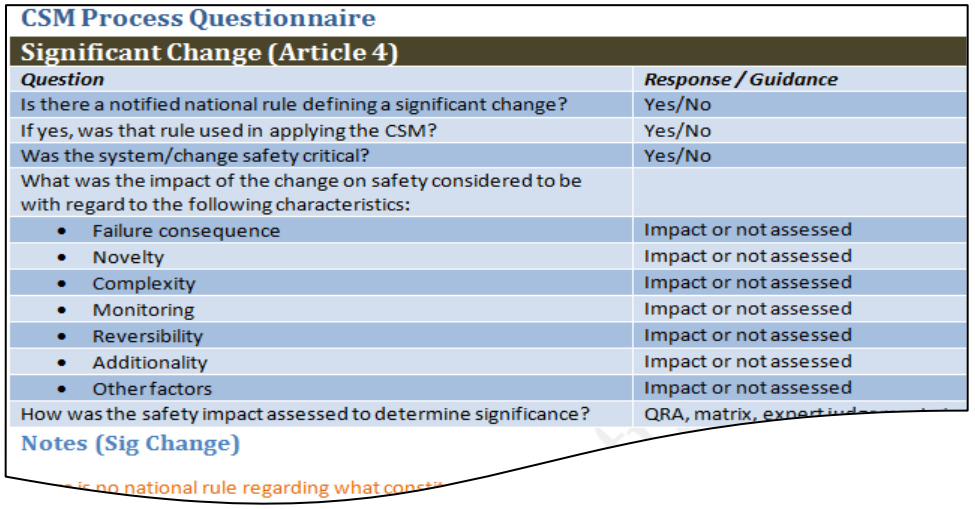
Some specific problem areas…

- What is a Significant Change?
- Selection of Risk Acceptance Principle.
- What level of detail should the Assessment Body consider?
- What should be on the Hazard Record?
- Is it different to what is done already?
  - In many countries the answer is generally ***no*** (including Norway). Processes already in place in existing safety management systems.
  - In some countries the concept of explicit risk estimation is not well embedded and this presents a challenge, as some form of risk assessment is required at several stages.



Significant Change

- There are no notified national rules.
- Dialogue between actors and NSAs etc. has created guidance in some countries (e.g. Great Britain and Austria).



CSM Process Questionnaire

Significant Change (Article 4)

Question	*Response / Guidance*
Is there a notified national rule defining a significant change?	Yes/No
If yes, was that rule used in applying the CSM?	Yes/No
Was the system/change safety critical?	Yes/No
What was the impact of the change on safety considered to be with regard to the following characteristics:	
• Failure consequence	Impact or not assessed
• Novelty	Impact or not assessed
• Complexity	Impact or not assessed
• Monitoring	Impact or not assessed
• Reversibility	Impact or not assessed
• Additionality	Impact or not assessed
• Other factors	Impact or not assessed
How was the safety impact assessed to determine significance?	QRA, matrix, expert judg

Notes (Sig Change)

is no national rule regarding what const

Example One

- The Engineering Department of a Railway Undertaking (RU) would like to increase the maximum speed limit of one class of passenger trains from 160 km/h to 200 km/h. This will eventually allow the merging of two rolling stock fleets into one.
- This is an Operational Change applied to Trains (Rolling Stock). The application of the risk assessment process to this change resulted in the definition of safety measures to control the hazards linked to it.
- There are thus two applications (also called iterations) of the risk assessment process: one for the operational change and one for the technical changes from the safety measures controlling it:
  - The operational change was considered as being not innovative, as it has been already in place in the proposer's organisation for other rolling stock (with the same bogies) and in other railway organisations. *It was however judged significant through dialogue with the NSA. (It is compulsory to liaise with the NSA who may require the application of CSM RA.)*

Example One (continued)

- For the technical change an assessment based directly on the criteria in CSM RA was applied.
- It requires an understanding of the railway hazards…
- Observations for consideration:
  - Could these hazards be generated as guidance for any change?
  - It is nearly always possible to argue that a safety consequence can result from a technical system failure and therefore all technical changes are significant:
    - Is it the before vs after situation that should be considered?
    - (In this case there is no equivalent “before” and so this observation doesn’t apply here.)

a) Failure Consequence: The worst case scenario associated with the failure of each of the technical safety measures was considered by the proposer:
   - Conical roller bearings: the worst case scenario for their failure is the blocking of the rotation movement between the shaft and the bearing box which can potentially lead to derailment.
   - Anti-Blocking System: the worst case scenario for its failure is its loss of function, which could lead to the creation of wheelflats which in turn could result in derailment,
   - Dampers (Shock Absorbers): The dampers' reference force is adjusted to the higher mass of the considered rolling stock. The worst case scenario for their failure corresponds to the simultaneous and complete loss of function of both dampers on the same bogie while the travelling speed is higher than the critical velocity. This in turn could lead to derailment.

b) Innovation: none of the modifications was considered particularly innovative, as they all have been used for many years in the proposer's rolling stock and elsewhere at 200 km/h operating conditions. (In particular, the shock absorbers are the same as those used on the Corail coaches and their reliability has been tested and tried successfully in that fleet. There is no issue regarding their geometry as they are fitted on identical bogies as the Corail bogies. The Anti-Blocking System has also been widely used in the proposer's Corail fleet. The same applies to the conical roller bearings)

c) Complexity: the modification consists in components that have been tried and tested for many years by the proposer. Its complexity was thus not considered to add additional risk.

d) Monitoring: Shock Absorbers and Anti-Blocking System are examined at each maintenance cycle, as are axle boxes and bearings, according to internal maintenance procedures. Anti-Blocking Systems are equipped with a diagnostic system and are tested at each train arrival and departure. Axle boxes temperatures are monitored by hotbox detectors on the infrastructure.

e) Reversibility: Any of the modification elements can be undone, restoring the system as it was before the change.

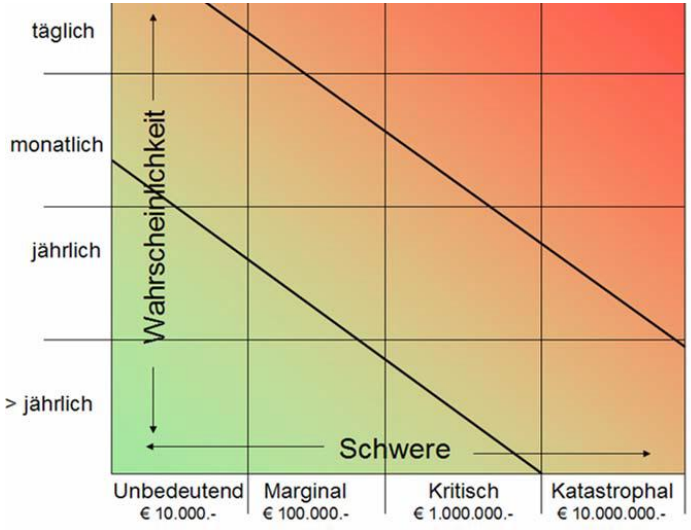
f) Additionality: No recent safety-related modifications were identified.

A failure of the system can result in major safety consequences (derailment). The change was thus considered significant based on Criteria a).

Example Two

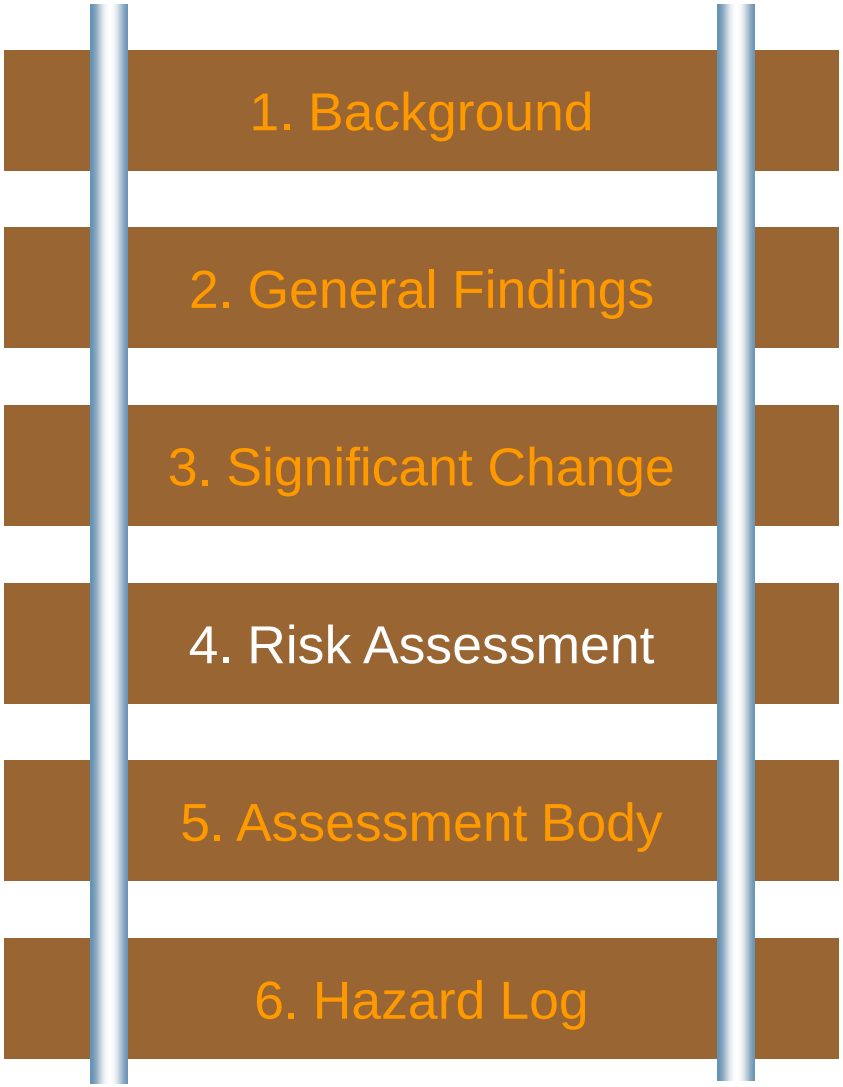
- The infrastructure manager has developed a flowcharted method for determining if a change is significant, as follows:

1. Are there any possible safety risks associated with the change? If **YES**, then:
2. Do the safety risks have an impact on a set of identified relevant accidents? If **YES** then:
   - Classify the impact of the change using a risk matrix.
3. Apply matrix criteria to determine if the change is significant:
   - If ***all*** hazards in green area then Not Significant – process as defined in organisation's SMS applied
   - If ***any*** hazard in red area then Significant and CSM RA applied
   - Risk Manager decision if amber



Example Two

- Observations:
  - More detail at the front end.
  - Concept of ALARP.
  - Requires development of appropriate decision criteria.
  - Requires list of hazards. (But this is a good thing – in my opinion!)
    - What are railway hazards?
    - What are hazard causes?
    - Derailment, SPAD, Fire, broken rail???
  - Requires agreement with NSA.

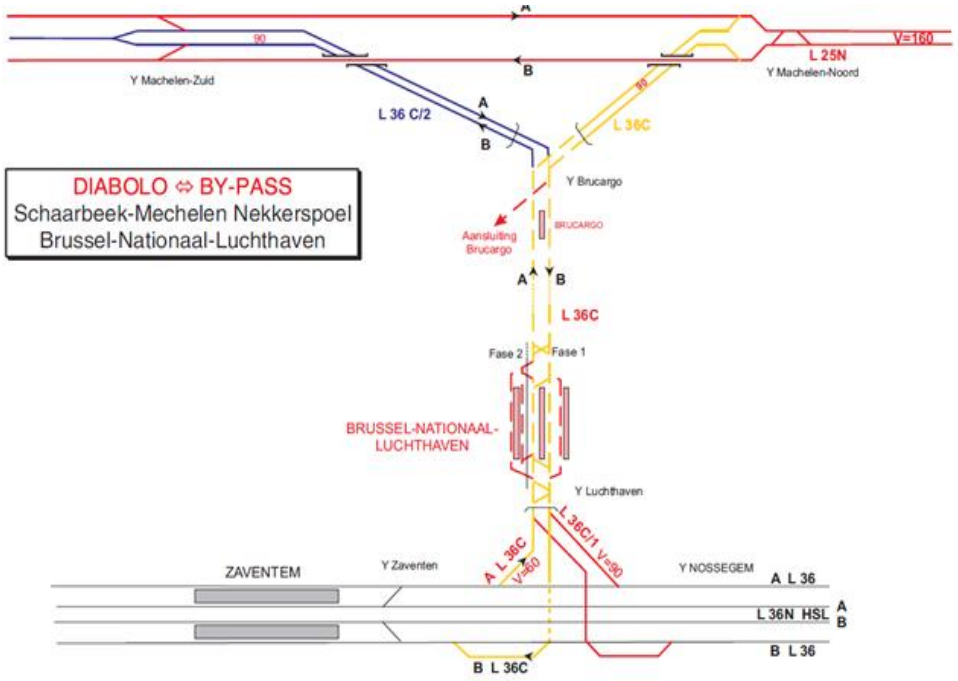


Selection of Risk Acceptance Principles

- General comments:
  - More subjective, little in the way of rules or guidance.
  - Normally done on a hazard cause by hazard cause basis.
  - Influenced heavily by the type or organisation rules based vs risk based regimes.
  - Some limitations have been applied to Similar Reference Systems:
    - Only SRS that are known and the actor has previous experience of.

Example One

- Added new infrastructure and modifying existing.
- The RAP for this change was selected as explicit risk estimation. The approach was adopted due to the complexity and novelty of the change.



Example One (continued)

Hazard	Zone	Unwanted event	Causes of dangerous situation	Consequences	Safeguards	Sev	L'hood	Risk Rank	Recommendations	Sev	L'hood	Risk Rank
fire on board a train	underground	Fire from a train in the tunnel	inattentive or careless travellers	dead (n) and/or seriously injured	Design of the tunnel: -fire-resistant cladding -fireproof cables -fire detection in technical premises -fire-fighting techniques (incl. smoke curtains) -evacuation paths and evacuation shafts -cross passage between the tubes, with fire doors -signalling-speakers-cameras-emergency phones-wireless communication system-building management system	6	2	8	Procedure for the possibility to continue until the tunnel exits or to the station, disabling the emergency brake control by travellers and with an evacuation procedure from the station	5	2	7
			Act of vandalism	damage to the railway system	Operation:-training and definition of the tasks of the staff located in the building management system, measures in case of incident, fire on board, in a tunnel: the driver should try to bring the train to a stop outside the tunnel; the train crew may fight the fire and, if necessary, stop the train and evacuate-				Procedure for adjusting the route of all trains near or in the tunnel in the event of a fire in the tunnel			

Example One (continued)

- Safety requirements become the list of safeguards and recommendations, extract:

Nr.	Safeguard	Resp. party
5	Extinguished “black” signal has the same meaning as a red signal aspect and implies that the train driver should contact the signal Tower	I-TN.22
6	Presence of people or animals in the track: train driver should horn and submit a report to TC or signal Tower as "persons in the track" which this imposes the procedure ' cautious driving "	I-TN.22
8	Fences at tunnel mouth side are equipped so that persons cannot enter the tunnel (fences on embankments along tunnel mouth)	I-I
15	Smoking ban	Holding
16	Reversing: Director will only authorise reversing after permission from signal Tower. There will be max. 1 train reversing.	I-TN.22
18	Emergency services will only intervene if assured them that there is no more operating trains	I-TN.22
21	Intrusion detection at tunnel mouths (and side station)	Holding
23	Procedure for evacuating incident train	I-TN.22
29	Operational Procedure for communication with different disciplines	Mitigation measures: I-N / Holding
	Etc.	

- Compliance is:
  - That there are no unacceptable risks according to the organisations risk acceptance criteria, which in turn means that the identified safety requirements are shown to be in place.

Example Two

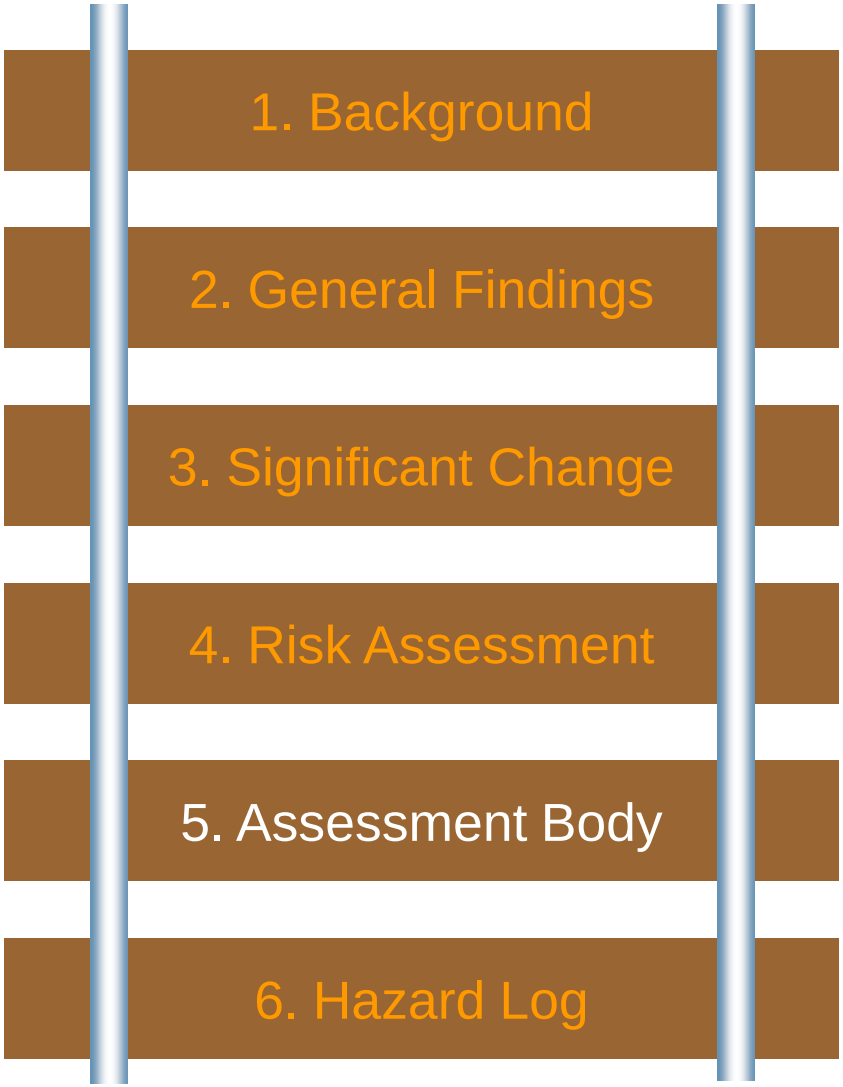
- The passengers transport function (the proposer in this example) of a Railway Undertaking (RU) would like to modify the wiring of the feedback loop controlling passengers' access doors on a high speed train. This is intended to reduce station dwell time and thus improve train and guard availability.
- This is a Technical change applied to Rolling Stock. In addition, this change has an operational element to it, as the operating instructions for train guards will be adapted to the new system characteristics.
- Hazards identified (for the technical change) were:
  - fire safety: fire hazard from the new cables and wiring layout,
  - electrical safety: electrical hazard from new cables and wiring layout,
  - door safety: hazard of doors closing/opening at the wrong times etc.
- For this actor, the hierarchy of selection of RAP is:
  - If relevant CoPs can be applied, then this is chosen as the RAP.
  - Otherwise, if comparisons with SRSs can be done then this is chosen as the RAP.
  - Otherwise, an ERE is carried out.

Example Two (continued)

- In this case it was decided that CoPs could address these hazards:
  - Addressing the fire hazard: National Standards for Rolling Stock Fire Behaviour and Selection of Materials: “General”, “Application to Electric Equipment” and “Provisions for Design and Fabrication”.
  - Addressing the electrical hazard: European Standard EN 50153 (Railway applications. Rolling stock. Protective provisions relating to electrical hazards) and UIC leaflets 533 (Vehicles, protection by earthing of metal parts), 550 (Power supply installations for passenger stock) and 552 (Electrical power supply for trains - Standard technical characteristics of the train line).
  - Addressing door safety: UIC leaflets 560 (Doors, footboards, windows, steps, handles and handrails of coaches and luggage vans) and 660 (Measures to ensure the technical compatibility of high-speed trains) and National Standards for “Mainlines passenger RS Footboards” and for Passengers access doors Characteristics, Operation, Control and Testing: “Passenger RS intended for running between 160 km/h and 220 km/h”, “Passenger RS intended for running on Urban and Suburban Networks” and “Passenger RS intended for running at speeds higher that 220 km/h”.

Example Two (continued)

- Compliance with the safety requirements is documented through:
  - components certificates (issued by manufacturer or certification body),
  - diagrams of the wiring layout,
  - fabrication procedures,
  - testing procedures,
  - adapted maintenance procedures.
- This evidence is part of the Modification Order. This is the file that formulates the definitive specifications for the modification (incorporating safety requirements) including an overview of the new wiring layout, a detailed circuit diagram, the identification of the components to be used, of the procedures (fabrication, testing, maintenance) to be applied and a modification to guards' operating instructions.
- In addition, letters between the different actors involved in the change, requesting or reporting the correct implementation of the Modification Order or parts of it (fabrication, maintenance etc.) also demonstrate compliance.
- The Assessment Body was part of the proposers organisation for this change.



Assessment Body

Detailed, including adequacy of measures OR Confirmation of process?

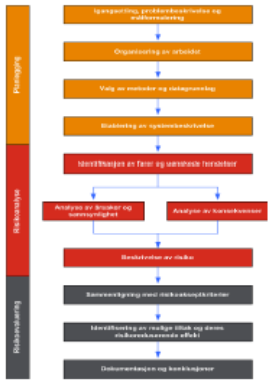
Evaluering av risikovurderingsprosessen

Hensikten med evalueringen er å kontrollere at man i utarbeidelsen av risikovurderingen har fulgt de elementene som kreves i NSBs beskrivelse av risikovurderingsprosessen. Hver fase av prosessen er beskrevet i de understående tabellene hvor innholdet fra kravdokumentet er gjengitt punkt for punkt.

I de tilfeller hvor kravet er delvis oppfylt eller ikke oppfylt, blir dette omtalt i kommentarfeltet under hvert element.

Et "Nei" i et av punktene vil ikke nødvendigvis føre til at evalueringen totalt sett underkjenner rapporten, men dette skal omtales i den endelige konklusjonen av evalueringen.

Risikovurderingsprosessen i NSB AS

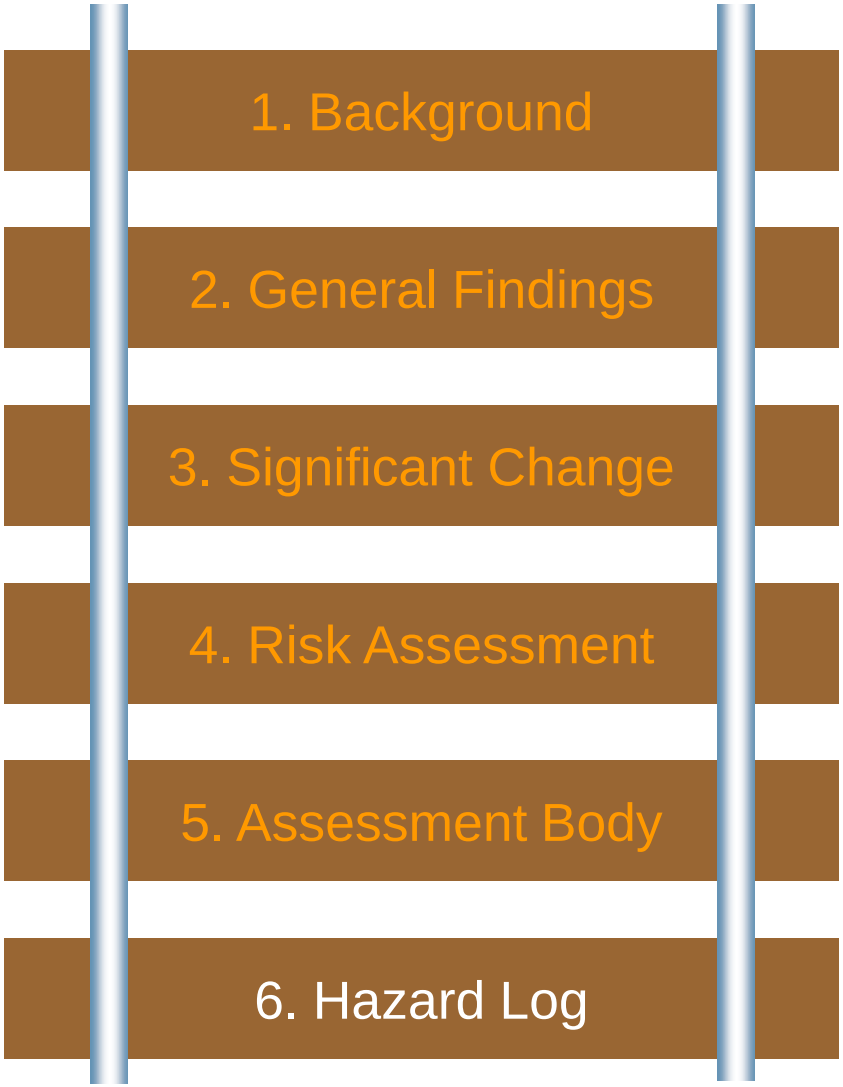


Planlegging		Ivaretatt Ja / Nei
	Er risikovurderingen registrert i Tiltaksplan trafikksikkerhet i Synergi, iht KD-00036?	Ja
	Har analyseleder etablert en analysegruppe som samlet har kompetanse til å ivareta alle aspekter av risikovurderingen?	Ja*1
	Er det utarbeidet en plan for utførelsen av risikoanalysen, i henhold til rammebetingelser gitt i oppdragsbeskrivelsen?	Ja*2
	Ble risikoakseptkriteriet valgt i planleggingsfasen og er dette egnet til evaluering mot den risiko som skal beskrives i risikoanalysen?	Ja
	Er det etablert en systembeskrivelse/beskrivelse av analyseobjektet i analyserapporten?	Ja*3

Kommentarer:
*1 Leder NSB Persontog var identifisert som personell som burde delta i arbeidsmøte i vedlegg 2 presentasjon av endringsanalyse- bakgrunn og prosess. Blant annet ut fra ledergruppens brede deltakelse i analysen deltok leder av NSB Persontog likevel ikke.
*2 Den valgte metodikken synes egnet til den aktuelle problemstillingen.
*3 Ligger som vedlegg til rapporten.

Assessment Body (continued)

- At present there is little guidance.
- New draft of CSM RA will provide more detail about:
  - Who can act as Assessment Body
  - Level of detail expected – requires some assessment of appropriateness of measures, hence towards the version on the left of page above.



Hazard Log…it's up to you!

Hazard	Zone	Unwanted event	Causes of dangerous situation	Consequences	Safeguards	Sev	L'hood	Risk Rank	Recommendations	Sev	L'hood	Risk Rank
fire on board a train	underground	Fire from a train in the tunnel	inattentive or careless travellers	dead (n) and/or seriously injured	Design of the tunnel: -fire-resistant cladding -fireproof cables -fire detection in technical premises -fire-fighting techniques (incl. smoke curtains) -evacuation paths and evacuation shafts -cross passage between the tubes, with fire doors -signalling-speakers-cameras-emergency phones-wireless communication system-building management system	6	2	8	Procedure for the possibility to continue until the tunnel exits or to the station, disabling the emergency brake control by travellers and with an evacuation procedure from the station	5	2	7
			Act of vandalism	damage to the railway system	Operation:-training and definition of the tasks of the staff located in the building management system, measures in case of incident, fire on board, in a tunnel: the driver should try to bring the train to a stop outside the tunnel; the train crew may fight the fire and, if necessary, stop the train and evacuate-				Procedure for adjusting the route of all trains near or in the tunnel in the event of a fire in the tunnel			

Hazard and cause	Risk Evaluation WITHOUT Additional Measures						
	Impact	Likelihood	Risk	Acceptable?	Hazard Basis	Responsible	Date
	Additional Measures						
	Risk Evaluation WITH Additional Measures						
	Impact	Likelihood	Risk	Acceptable?	Hazard Basis	Responsible	Date

Nr.	Operation Location	Unit person							
Date	Title	Reviewer	Nr.	Action Description	Action Comment	Responsible for measures	Deadline	Status	Performed
94923 11.03.2011	Risk assessment of new organizational structure		1	Prepare the assignment description for the implementation of the change analysis.	The mission description is prepared and signed by the Director of Passenger train operations.		13.04.2011	Performed satisfactorily	10.04.2011
			2	Measures 1. Clarify the roles and responsibilities of the various entities in respect of traffic safety	Roles and responsibilities are clarified. Any changes to the law to be clarified in the evaluation which is to take place within 6 months of the change. VK-000294 overview of traffic safety forums, feature descriptions and organization charts are updated.		01.06.2011	Performed satisfactorily	01.06.2011
			3	Measures 2. Define traffic safety interaction forums, mandate, participation and decision making	VK-00294 overview of traffic safety forums are updated and approved in the meeting for 7.6.2011. Any changes to the law to be clarified in the evaluation take place within 6 months after the change.		01.06.2011	Performed satisfactorily	01.06.2011
			4	Measures 3 preparation of where and how traffic safety and HR training issues fit into the existing forums or if it creates new requirements.	A working meeting regarding the above has been arranged and a final conclusion taken in management meeting of "Passenger train". A decision was made to		01.06.2011	Performed satisfactorily	01.06.2011

Hazard ID	Hazard/sub-hazard	Hazard cause	Hazard cause	Operating Mode	Location	System	Subsystems	Type	Interfaces with	ADCs	Accidents/Top Events	Initial Consequence	Initial Frequency	Confirmed RRN	Possible new RRN	Actions/RRN	Responsible	Comments	Status	Date added	Date updated	Residual Consequence	Residual Frequency	Closed
H1	The Signalling System contributes to an excessive steering value to a train						Signalling System	Conventional / ERTMS									Unnamed Project		Open					
H1.01	The Signalling System sends an excessive steering value to a line side signal.						Signalling System	Conventional			1, 2						Unnamed Project		Open					
H1.02	The Signalling System sends an excessive steering value to train via GSM-R						Signalling System	ERTMS			1, 2						Unnamed Project	Ev. can de less restrictive rules are used	Open					
H1.03	The Signalling System sends an excessive steering value to the ATC balise.						Signalling System	Conventional			1, 2						Unnamed Project		Open					
H1.04	The Signalling system sends an excessive steering value to a avalanche signal.						Signalling System	Conventional / ERTMS			2						Unnamed Project		Open					

Summing up

- Still embryonic.
- Not applied in several countries.
- Not too different to existing practices in Norway, excluding the significant change and assessment body. Perhaps also the Code of Practice approach is not used very often in Norway.

The End – Any Questions

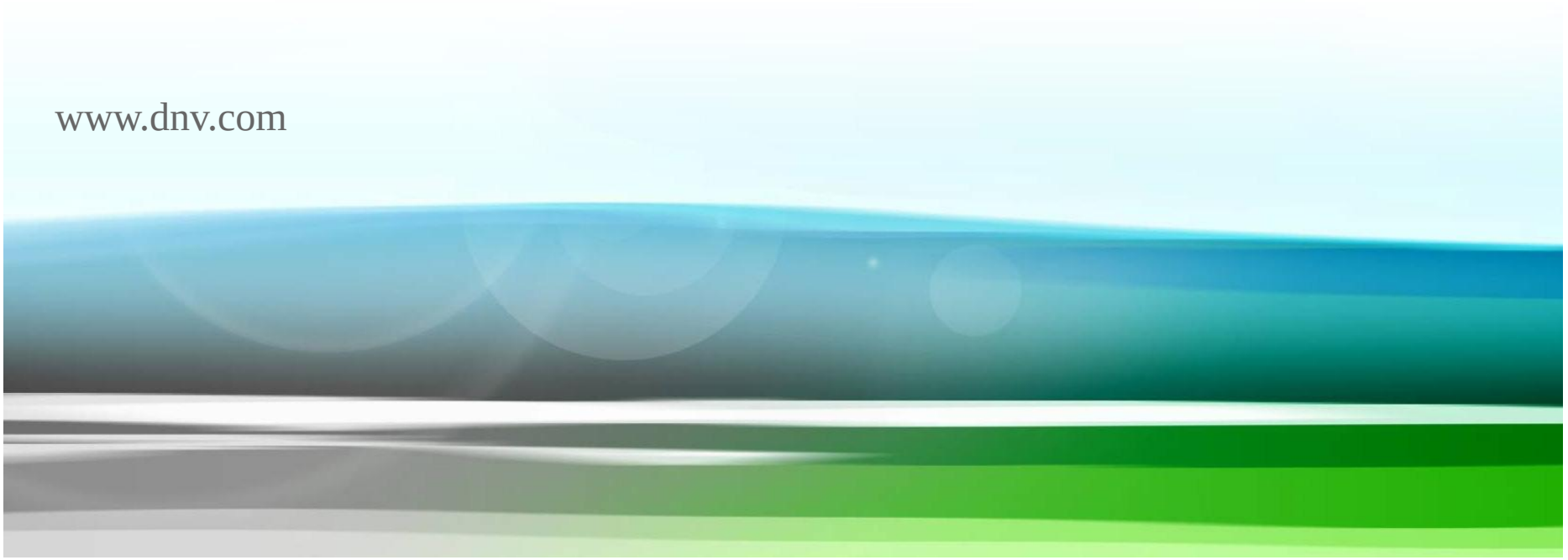
Projects with ERA

- Risk Acceptance Criteria used in Industry:
  - What other industries do in relation to the question “how safe is safe enough”?
  - *Could have relevance to risk acceptance / explicit risk estimation parts of CSM.*
- Safety Performance Indicators used in Industry.
  - Monitoring of accident / incident precursor information and how this is used.
- Freight Train Derailments: Mitigation Measures:
  - Detailed assessment of the causes, consequences of freight train derailments.
  - Compilation of prevention measures that exist now and which may be introduced to the market in future (precursor to EU D-Rail project).
  - Cost-benefit analysis of above.
  - *Could be considered an example of a detailed explicit risk estimation.*
- Collection of Examples of CSM RA. Just reaching completion.
- ERTMS “human factors” framework. No activity.
- Research into Risk Regulation processes. Just started.

Search “DNV” on ERA’s web-site for links to studies.

Safeguarding life, property and the environment

www.dnv.com



MANAGING RISK