Proceedings of the RSII 2012 Seminar on Rail Safety & Incident Investigation
April 30 – May 02, 2012, Orlando, Florida, USA

COMPLIANCE VS RISK ASSESSMENT: WHEN HAVE WE DONE ENOUGH?

Howard J. Parkinson
Chartered Engineer
BSc(Hons) MSc PhD CEng MIMechE MIRSE PGCE
Progressive Assurance LLC
hjparkinson@railsystems.co.uk

ABSTRACT

In the UK railway it is necessary to show that risks relating to any design solutions are ALARP (as-low-as-reasonably-practicable). It is a legal requirement and in certain instances complying with a standard may be enough; however in other circumstances we may have to perform a formal risk assessment. It seems clear that there is a continuum between the two positions but how do we know what to do and if that is enough? This paper seeks to address this matter. UK risk acceptance including the ALARP principle is explored and compliance versus risk assessment, including standards, is discussed. An example of a compliance safety process is given using a case study based upon changes to rolling stock. A further example where risk assessment and a cost benefit analysis have been employed to support a safety argument for a non compliant gradient in a siding is then presented followed by concluding remarks.

Keywords
Risk Acceptance, ALARP, Compliance, Risk Assessment, Cost Benefit Analysis.

1. INTRODUCTION

It is a legal requirement In the UK railway to show that risks relating to a particular design solution are ALARP (as-low-as-reasonably-practicable) [**Error! Reference source not found.**]. Complying with a standard may be enough to do this; however in other circumstances we may have to perform a formal risk assessment. It seems clear that there is a continuum in between these positions but how do we know what to do and if that is enough?

This paper seeks to address this matter. Section 2 discusses UK risk acceptance including the ALARP principle and explores some of the consensus surrounding the principle. Section 3 discusses the compliance versus risk assessment continuum. Section 4 presents an example of developing a process for accepting a compliance safety argument using a case study based upon changes to rolling stock. By demonstrating compliance against standards and ensuring the suitability and sufficiency of these standards to the design option in question, ALARP can be demonstrated. To use this approach, the standards must be current and cover all the hazards faced. The issues of compliance and risk assessment are discussed and general rules are derived. By understanding this paradigm, lower risk changes can be made more efficiently.

Section 5 presents an example where risk assessment and a cost benefit analysis have been employed to support a safety argument. The example is a situation where a analysis could be employed to support an ALARP argument for a non compliant gradient in a siding. Conclusions and closing remarks are made in Section 6.

2. RISK ACCEPTANCE AND ALARP

The Railway Standards and Safety Board (RSSB) document, “Taking Safe Decisions” [1] sets the consensus on risk acceptance in the UK and is based upon extensive research and the soliciting of industry expert opinion over several years. The primary piece of

legislation in the UK relating to Health and Safety is the Health and Safety at Work Act 1974 [2] and this legislation is where the concept of ALARP comes from. The act does not actually mentioning ALARP directly but SFAIRP. The quotation from the Act is

"2.-(1) It shall be the duty of every employer to ensure, so far as is reasonably practicable (SFAIRP), the health, safety and welfare at work of all his employees.
3.-(1) It shall be the duty of every employer to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not thereby exposed to risks to their health or safety".

There are other clauses that also refer to SFAIRP. In this paper when ALARP is referred to it means the same as SFAIRP. Some sources make a differentiation between SRAIP and ALARP, supposing that if followed they give differing outcomes in terms of how onerous they are respectively for no logically clear reason, however, the consensus based upon the RSSB [1] is that the two concepts mean exactly the same thing.

Other countries have different risk acceptance approaches, for example the GAMAB (Globelment au Moins Aussi Bon) that is used in France and basically requires that *"All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system"* [3]. Countries other than the UK such as Australia and New Zealand use the ALARP principle in a very similar, if not identical, way to the UK. Several countries that build new Railways use contractual requirements that ALARP is demonstrated, for example in Hong Kong, Saudi Arabia or The Netherlands. In Germany there is the concept of Minimum Endogenous Mortality (MEM principle) "Hazard due to a new system would not significantly augment the figure of the minimum endogenous mortality for an individual" [3] but there are still discussion taking place about the application of this principle and it is not currently widely used in rail.

When taking safety decisions and seeking to demonstrate ALARP *"…a computation must be made…in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other"* [5]. Thus it is a balancing act and how this balance can be made is discussed in Section 5.

This means that a suitable and sufficient assessment of any risks must be made, comparing the cost of implementing risk control measures against the reduction in risk. But must we always have to make a risk assessment when we have competent people employing comprehensive standards? That is answered below in Section 4.
This is all based upon what is considered reasonable; for which the legal system is the ultimate arbiter based upon the longer term needs of society. The demonstration that the risk is ALARP can be done in various ways depending upon the level of risk, and the size and complexity of the change. The UK good practice guidance on engineering safety management, "The Yellow book" [7] states that analysis undertaken should be "commensurate with the level of risk and complexity of the change proposed".

A lot of misconceptions exists [6] regarding ALARP which is basic tenet of English safety law. Some of these misconceptions are described in the following section.

There is confusion about what is commonly referred to as the ALARP diagram. The diagram showing the so called ALARP diagram (inverted triangle) as shown in Figure 1 is often quoted during discussions of the ALARP principle. This diagram shows unacceptable, tolerable, or broadly acceptable regions demarcated by horizontal lines annotated with quantified targets of say $1x10^{-5}$. Different diagrams have slightly different labeling but the idea is the same. This is a Tolerability of risk diagram and is not an ALARP diagram.

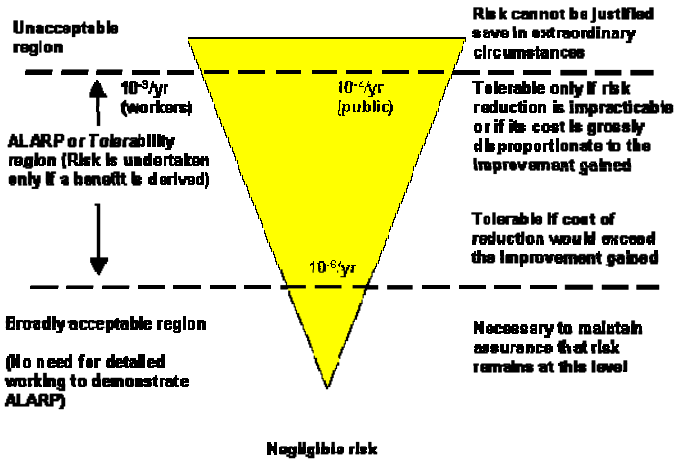

Figure 1 Tolerability of Risk

[http://www.hse.gov.uk/comah/assessexplosives/step5.htm]

The horizontal lines of risk shown are for individual risk to different population exposed to the risks from the railway per person per year, which are set by the government or safety regulator to reflect societal concerns. Taking Safe Decisions [1] explains that collective risk is how projects perform the risk assessment and there is no legal requirement for a company to prove that the individual risk to passengers or workers is at a particular level i.e.

tolerable or negligible, merely to show that they are ALARP. Companies may want to do more than is required by the ALARP principle and/or demonstrate individual risk levels for sound business reasons but they are not legally obliged to do so. Legally ALARP is the only test for an Infrastructure Manager or Trainer Operator in the UK. Collective risk and Individual risk are defined as [1].

"The collective risk is the aggregate risk, possibly to a range of different exposed groups, associated with a particular scenario, control measure or hazardous event. Collective risk can be quantified as the average number of fatalities, or fatalities and weighted injuries, per year that would be expected to occur. When undertaking an assessment of whether or not a measure is necessary to reduce risk to a level that is ALARP, the change in risk associated with the measure is a collective risk estimate".
and
"Individual risk relates to the probability of fatality per year to which an individual is exposed from the operation of the railway. Individual risk is a useful notion when organizations are seeking to understand their risk profile and to prioritize and target safety management effort. The Office of Rail Regulation (ORR) categorizes individual risk as 'unacceptable', 'tolerable' and 'broadly acceptable' for the purposes of prioritizing and targeting its enforcement activity"

The latest version of Yellow Book [7] creates some confusion in this respect and mixes up individual risk and collective risk which leads one to the conclusion that this is probably a potentially confusing subject. There has had to be a Corrigendum [8] to the Yellow Book issued which states

"…. when reaching a decision as to whether you have met the obligation in the Health and Safety at Work Act (etc) 1974 to reduce risk to a level which is as low as reasonably practicable (ALARP), you do not have to:

- *divide risk into broadly acceptable, tolerable and intolerable regions and treat risks differently according to which region they fall into; or*

- *take account of any societal concern about risk. Societal concerns are an input to government decision making but other parties are not legally obliged to take them into account"*

The guidance to the widely used European safety standard, EN50126-2 [4] is incorrect in its interpretation of the ALARP principle using individual risk targets to make a case for safety in an example.
Another common misconception is the value placed upon a life lost in an accident involving many fatalities should be higher to reflect the aversion of society to large accidents.
The study report, "The Route to Safe Decisions" [9] states,

"The study found that there were no scenarios identified for which those surveyed believed that a figure higher than the VPF should be applied. The research found that: the value attributed to a multi-fatality accident was no higher than that attributed to the equivalent number of single fatality accidents the value attributed to accidents thought to inspire dread (for example death in a fire) is not higher than any other. Therefore this indicates that there is no justification for scaling up the VPF to take account of societal values since they are already taken into account in the existing value. It is therefore logical and sensible to use the accepted VPF value in all such circumstances".

The European railway safety standards EN50126-1 [3] is out of line with this current interpretation of the ALARP principle. It advises that the line in the graph showing the tolerable region can be sloped to take into account this aversion to large accidents. The dislike of large accidents is termed "Differential Risk Aversion" (DRA)".

A key point with the ALARP principle is that a whole life safety view should be taken. The demonstration of safety needs to be viewed over the entire lifecycle of a product or project. If the overall benefit of a safety system results in a minor safety disadvantage over a short migration period that is outweighed by the whole lifecycle safety benefit, this should not stymie the initiative [10];

It must be noted that **all** risk should be reduced to ALARP. Even with a very low the risk level it is incumbent to accept any safety improvements that can be made for minimal cost. Companies can also use the ALARP principle to remove unnecessary risk control measures that may have been supplemented or superseded.

3. COMPLIANCE VERSUS RISK ASSESSMENT

When we have to demonstrate the safety of railway systems such as rolling stock or command and control systems, we have various tools at our disposal. The processes we can use are laid down in standards EN50126-1 [3], and guidance such as The Yellow Book [7]. These recommend tools and techniques for assuring safety and by following them throughout the product and project lifecycle we can develop a safety case which comprises all the assurance evidence that has been produced. Within these standards and guidance there are triggers for conducting risk assessments. As stated previously, In the UK railway it is necessary show risks relating to any design solutions are ALARP (as-low-as-reasonably-practicable). ALARP is a legal requirement

and complying with a standard may be enough; however in other circumstances we may perform a risk assessment. It seems clear that there is a continuum with a formal risk assessment at one end and a compliance argument at the other, but how do we know what to do and if that is sufficient?

The latest version of the Yellow Book [7] deals with this issue but does not give any useful examples. The Yellow Book Application Note [12] deals with this issue in more detail but also does not any give useful examples. Figure 2 below developed by the Author provides a useful diagram that helps with an understanding of the issues involved.

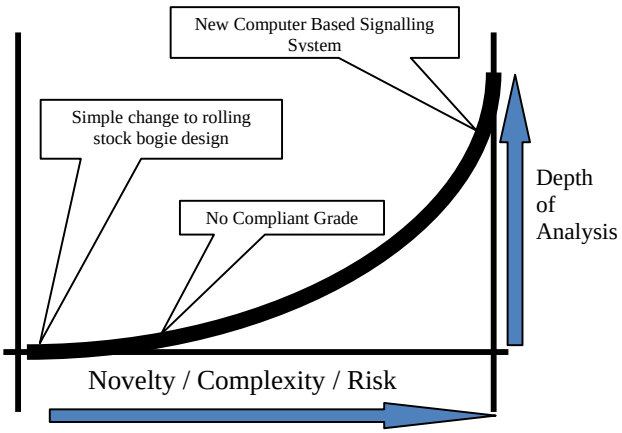

Figure 2: Risk Continuum

Many ALARP demonstrations would not be at one end or the other of the continuum but would probably involve some risk assessment and some argument that particular standards have been complied with.

A novel computer based interlocking would be towards one end and would mean that a full formal risk assessment processes as laid down in EN50126-1 [3] would be invoked. At the other end could be a safety decision regarding changes to a rolling stock mechanical component for which rigorous interfaces standards exist.

4. A COMPLIANCE BASED SAFETY ARGUMENT

By demonstrating compliance against standards and ensuring the suitability and sufficiency of these standards to the design option in question, ALARP can be demonstrated. To use this approach, the standards must be current and cover all the hazards faced. The following example based upon changes to rolling stock, illustrates how one might go about setting up a decision framework. It must be borne in mind that because drafter of the standards cannot predict every eventuality, they must be employed judicially and with common sense. The following quotation comes to mind

"Rules are for the obedience of fools and the guidance of wise men" Group Captain Sir Douglas Bader, RAF WW2 Fighter Ace

It is impractical and unnecessary to risk assess every application of every standards to demonstrate ALARP. Engineers as part of their job have always implicitly risk assessed their decisions and if they document their rationale in applying a particular standards then that could be sufficient given certain caveats.

Standards can be mandatory or may represent good practice. Some standards such as British Standards are not usually mandatory in the railway but represent good practice. Examples of mandatory standards that define railway functional interfaces for rolling stock, signaling and infrastructure include, UK, Railway Group Standards [13] or in Australia, Minimum Operating Standards [14] or across European networks, the Technical Specifications for Interoperability (TSI)s [15] .

Standards can be of more or less authority depending upon the way they are drafted and reviewed. The key criteria are that the standards must be kept up to date and operational feedback and accident data must be regularly reviewed. There must also be a means by which it is guaranteed that interface standards are complied with.

It is the case that a system or component can be compliant yet unsafe. An example of this happened in the UK where parameters for lateral and vertical track deviation were within those laid down in track standards yet some unloaded freight wagons (particularly short ones) were derailing even though they were adequately maintained. The problem was known as cyclic top and has been subsequently modeled and the standards and monitoring procedures amended.

It must be noted that complying with certain standards can sometimes stymie creativity and optioneering and optimization opportunities. Also, compliance with standards will not provide a defense against incompetence.

The following example involves a railway company that is both the infrastructure manager and a train operator that also allows access to its infrastructure to third parties operators on the shared railway.

The company has an extensive set of minimum operating standards (MOS) that define the safe interface requirements for rolling stock running on its system. These MOS include rolling stock kinematic envelopes, track gauge, wheel size, braking rates, pantograph requirement, train lengths, wheel profiles, etc. The company has a very involved safety management system that requires all changes to the infrastructure or rolling stock to undergo a risk assessment in order to determine whether the risk is ALARP. This could result in an onerous and potentially unproductive use of resources. It would make sense to have an approved change process that would allow lower risk changes, provided they fulfill certain criteria, to be made on the basis that they comply with the MOS.

The Yellow Book Application Note [12] gives the following advice regarding the making of a compliance based safety argument

"Before you decide that just referring to standards is enough, make sure that:

- *the equipment or process is being used as intended;*
- *all of the risk is covered by the standards;*
- *the standards cover your situation; and*
- *there are no obvious and reasonably practicable ways of reducing risk further."*

The point being that the standards must cover the risks i.e. they are suitable and sufficient. Standards could be several years old and may not cover some newer technology for example. When relying on compliance to a standard to demonstrate that the solution is suitably safe, the bulleted points should be judicially considered and the outcome recorded. If there is any doubt then some form of further risk assessment would normally be needed.

So in order to establish an approved safety change process, the first thing to do is to ensure that the standards cover the situation, i.e. the changes to the rolling stock or new rolling stock. A risk assessment workshop using subject matter experts and key stakeholders should be convened. A list of typical rolling stock hazards can then be reviewed. These must be comprehensive and relevant to the particular domain, for example in Saudi Arabia, sand could be a hazard, in Canada, snow, in Australia, bush fires. Standards usually do not specifically list the hazards that they control, this is often implicit.

The workshop would cover four main areas:

1. Review of known risk controls from operational data.
2. Identification of risks/controls not already captured.
3. Review of generic hazard data available from the national safety authorities.
4. Review of the rolling stock approval processes to ensure that its management does not introduce unreasonable risk in terms of operational feedback, updating and maintenance.

It is likely that some unforeseen risks or new risk could be identified and these will need to be updated in the standards as soon as possible. After this first stage it will be possible to ascertain that the risks are coved by the standards.

The standards must be applied by competent expert practitioners, or if in organization where this expertise is not widely devolved there must be a means by which decision making is adequately controlled.

Competent experts must underwrite risks in organizations. That is why they need to train as engineers, go to college, get involved in Continuing Professional Development (CPD, become members of Institutions, to enable them to have the competency set to underwrite risk. They take safety related decisions. This is sometimes forgotten and this results in bloated decision making by committees [10].

To complete the approved safety change process, any acceptance process paperwork should then be reworded. This should ask the engineer, when he is making the compliance based argument for safety and not invoking the companies risk based processes laid out in the safety management system, if the bulleted points can be answered in the affirmative and why. It is important to keep a record of any decisions and rationale.

5. RISK ASSESSMENT CBA

If we need to depart from established good practice and standards, then some form of formal risk assessment is probably required. Given that a risk based argument is necessary, how do we make an ALARP justification and how do we know that we have done enough to make the system sufficiently safe, or for that matter too safe? What does the demonstration of ALARP actually involve, especially when risk assessment is being used?

Using an examples, this section discusses an ALARP solution based upon risk assessment using structured expert judgment and Cost Benefit Analysis (CBA).

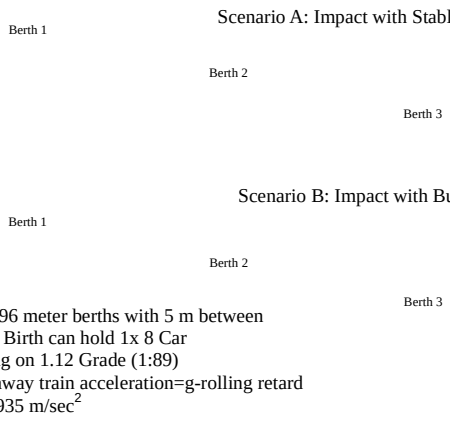

Figure 3: Impact Scenarios

In this example a non-complaint gradient in a stabling facility which is part of a major area upgrade is used as shown in Figure 3.

As part of the derogation process against a non compliance, an assessment of risk is required. This example shows how a risk assessment and cost benefit analysis can be employed to support an ALARP argument. It is often in the case in the railway that we must justify our decision making based upon risk assessment and the likely benefits of a change even though sometimes it may seem obvious that a design decision can be justified on the trade-off between risk and cost. Where safety is concerned, if the argument to be made is to support not spending money or spending money elsewhere, special care and scrutiny must be applied and a comprehensive argument must be made to support a decision.

It has been estimated that it would cost 10 million to make the grade compliant with standards. In order to justify not spending the money the delta risk between the compliant and non compliant grades would have to result in a safety benefit that was not grossly disproportionate to the cost of the measurer i.e. the civil works to make the grade compliant.

For arguments sake, let us assume that the rolling stock being stabled are relatively old stock that lack automatic parking brakes and therefore could rollway if the manual parking brakes are not applied, which is a known problems. The stock is parked in birth 1 at the top of the hill whilst it is being decanted and cleaned by cleaning staff.

The number of times a train rolls away per year has been discussed by a risk workshop. A figure of approximately 2 rollaway of train every five years from non appliance of parking brakes, was estimated as the frequency across the network and this is backed up by the data. From the number of vehicle in the fleet, the probability of a particular train rolling away can be extrapolated per birthing.

The risk is to cleaning staff who could be on the train when it rolls away and either collides with buffer stops or another train. Scenario B, colliding with buffer stops should not have a material effect on the risk to the cleaning as there will be retarding buffer stops that are designed to cope with this scenario. The risk is when the roll away train collides with a stationary train birthed in 3, scenario A. The speed of impact will be higher for the steeper non compliant grade. The speeds are calculated using basis physics and knowledge of the rolling resistance. A complying grade has an impact of velocity 20 km/hr, with the existing grade 28 km/hr resulting in a likely major injury rather than minor (estimated). The consequence is difficult to assess however there have been studies done on the design of railway vehicle interiors.

The factors that need to be assessed in order to understood the risk for both the non-compliant and compliant grades are

- the probability that a train will roll away,
- the likely impact speed,
- the number of personnel exposed
- the probability that the personnel are exposed and, the consequence for the exposed personnel.

From the calculation the delta risk which comes out at 7.43E-05 equivalent fatalities per annum. From this we can assume a safety benefit per annum based upon the Value Per Fatality (VPF). Now we must work out the cost amortized over the design life of the upgrade. UK Health and Safety Executive (HSE) guidance [16] is useful in this matter. A rough calculation can be made by multiplying the safety benefit over the design life of the project. A more involved study can be made using a spread sheet for calculating the costs of capital calculations, depreciation and discounted cash values. The end result of using the spread sheet or doing a rough and ready approach is not significant in this case but it is recommended to undertake a sensitivity analysis varying some parameters to ensure this is true.

Other Personnel being hit by a rollaway train has not been considered for assessment as the risk delta between the compliant and non complaint grades would not be significant as the probability occurrence and the consequences would be very similar.

Other assumptions that have been made are:

-The trains will be decanted and moved down to Berth 2 after 1 hour (estimate). This is the time when there is the opportunity for the train to rollaway and hit the train already berthed in Berth 3.
-Calculations of rollaway speed based on all brakes coming off at once.
-Brake leak off is more likely to occur 1 to 24 hours after the train is stabled without the Spring Parking Brake applied and the Master Controller is cut out. If the rollaway occurs with some brakes still engaged say 10-40% only low accelerations would result. For this analysis it assumed all brakes release at once. Assuming that the brakes could come off at any point from being stabled, however this is very pessimistic as they would probably only come off after several hours.
-A major injury = 1/10 of a statistical fatality [16]. A minor injury = 1/200 of a statistical fatality [16].
-The VPF(value to prevent a fatality) used = 3.5×10^6 Dollars (a realistic figure based upon the UK)
-Gross disproportion was discussed earlier. The figure for gross disproportion is 5 however this must be agreed with stakeholders.

The following assessment can be made.

ALARP Assessment		
Cost of fatality =	$3,500,000	
DELTA Risk of fatality per year =	7.43E-05	
Annual Cost of fatality with DELTA risk =	$260	per year
MAX Reasonable annual spend to avoid fatality is 5x annual fatality =	$1,300	per year

Any other possible mitigations must also be considered including a review the design options for decanting and stabling. The possible design measures that could be employed to mitigate the rollway risk could be: to modify rolling stock so that they have automatically applied parking brakes: increase the number of sidings so that none are containing more than 2 berths or to provide decanting on first 2 berths: add derailers or piston retarders: the driver to place chocks under wheel in berth 1 (Not recommended for safety reasons).

All these practicable solutions came in with a cost ranging from $10 000 to several million dollars and are not reasonably practicable using the ALARP criteria. There are no engineering solutions with costs under $10,000 per year and therefore the existing risk meets ALARP principle. i.e. to make the grade compliant is not a reasonably practicable measure. No additional design controls were identified that were reasonably practicable to implement. It is important to note that the quantified figures should only be used as an input into the decision making process and should not be used to replace expert judgment.

6. CONCLUSION

The ALARP principle has been explained and common misconceptions have been identified. The continuum upon which compliance and risk assessment safety arguments reside has been identified and discussed. Examples have been given of instances when differing approaches are necessary and how risk acceptance criteria are appropriate.

It must be stressed that in all the work described, structured and judicial application of expert judgment is vital for the safety of the railway.

REFERENCES

1. Taking Safe Decisions: ref: GD-0001-SKP © RSSB 20
2. UK Health and Safety at Work Act 1974
3. EN50126-1: The specification and demonstration of reliability, availability, maintainability and safety (RAMS)
4. EN50126-2: Guide to Railways-Applications S&D RAMS - _safety (February 2007)
5. All England Law reports, Edwards vs. National Coal Board, 1949, vol. 1, pp. 743-749.
6. An Independent Review. The Loss of RAF Nimrod in Afghanistan in 2006. Hadden Cave Report ISBN: 9780102962659
7. Engineering Safety management (The Yellow book 4), ISBN 978-0-9551435-2-6
8. Yellow Book Corrigendum
9. Route to Taking Safe Decisions
10. IRSE Guidance on the Application of Safety Assurance May 2010
11. Processes in the Signalling Industry
12. Yellow Book Application Note 8 “Safety Management and Standards”
13. RSSB Group Standards www.rssb.co.uk
14. RailCorp Minimum Operating Standards www.railcorp.mos.gov.nsw.au
15. European Technical Specifications for Interoperability www.era.eu
16. Health & Safety Executive Guidance publication, *Reducing Risks Protecting People* (2001*)*