Chapter 2

A Systems View of Railway Safety and Security

Ali G. Hessami

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/62080

Abstract

This chapter approaches the concerns over safety and security of modern mainline and light railways from a systems perspective. It addresses the two key concerns from the view point of systemic emergence arising from the interaction between all the principal constituents of the railway system, namely infrastructure, rolling stock, energy and human element comprising workers, passengers and the neighbours of the railways.

It presents a system level perspective on the requirements of the railways that impact on all design, development, operations, maintenance and upgrades. It offers a classification system for the requirements that includes safety and security concerns amongst in excess of twenty other requirement categories. The chapter subsequently covers a whole railway safety study carried out in the United Kingdom that is the only example of such analysis globally and will give an overview of the findings of this holistic safety study that may provide a reference for all international mainline railways.

Finally, the chapter reviews the trends in railway safety and security, and the impact of new control and command technologies on the safety performance of railways including a view of the emerging issues.

Keywords: Railway safety, Railway security, Railway system, Requirements, Emergence

1. Introduction

Modern railways have moved a long way from the slow, noisy, polluting and poor safety record of their earlier ancestors and offer speed, comfort, convenience and enhanced safety approaching those of air travel these days. This is largely driven by incorporation of many modern innovations into the infrastructure, rolling stock and operations comprising advanced computing on-board and track side, high-speed communications, energy efficient traction

systems and new track materials. These evolutionary changes have rendered railways a highly attractive mode of transportation in today's world.

2. A Life-cycle Perspective

The systematic safety assurance of a product, system or process (PSP) requires the consideration of key activities at each phase of the development and deployment. This is referred to as the life-cycle perspective and constitutes the backbone of the most standards and codes of practice.

The generic PSP safety life-cycle comprises 12 phases as follows:

1. Concept Definition

2. Detailed Definition and Operational Context

3. Risk Analysis and Evaluation

4. Requirements (including Safety Requirements) Specification

5. Architecture and Apportionment

6. Design and Implementation

7. Manufacture/Production

8. System Integration

9. Validation

10. Acceptance

11. Operation, Maintenance and Performance Monitoring

12. Decommissioning.

The life-cycle concept constitutes the backbone of the systems engineering practice and the most system safety processes, standards and codes of practice. It exists in a variety of forms and detailed stages depending on the source. One old reference from railway safety standards [1,2] depicts this as a 12–14 phase process by separating many of the later stages such as monitoring and modification into distinct phases as depicted in Figure 1.

3. System Level Requirements and Classifications

The starting point of a comprehensive understanding of a desired or existing system is the so-called system level perspective. Once a level of interest in the hierarchy is stated, then the clear description of the system is the principal starting step.

http://dx.doi.org/10.5772/62080

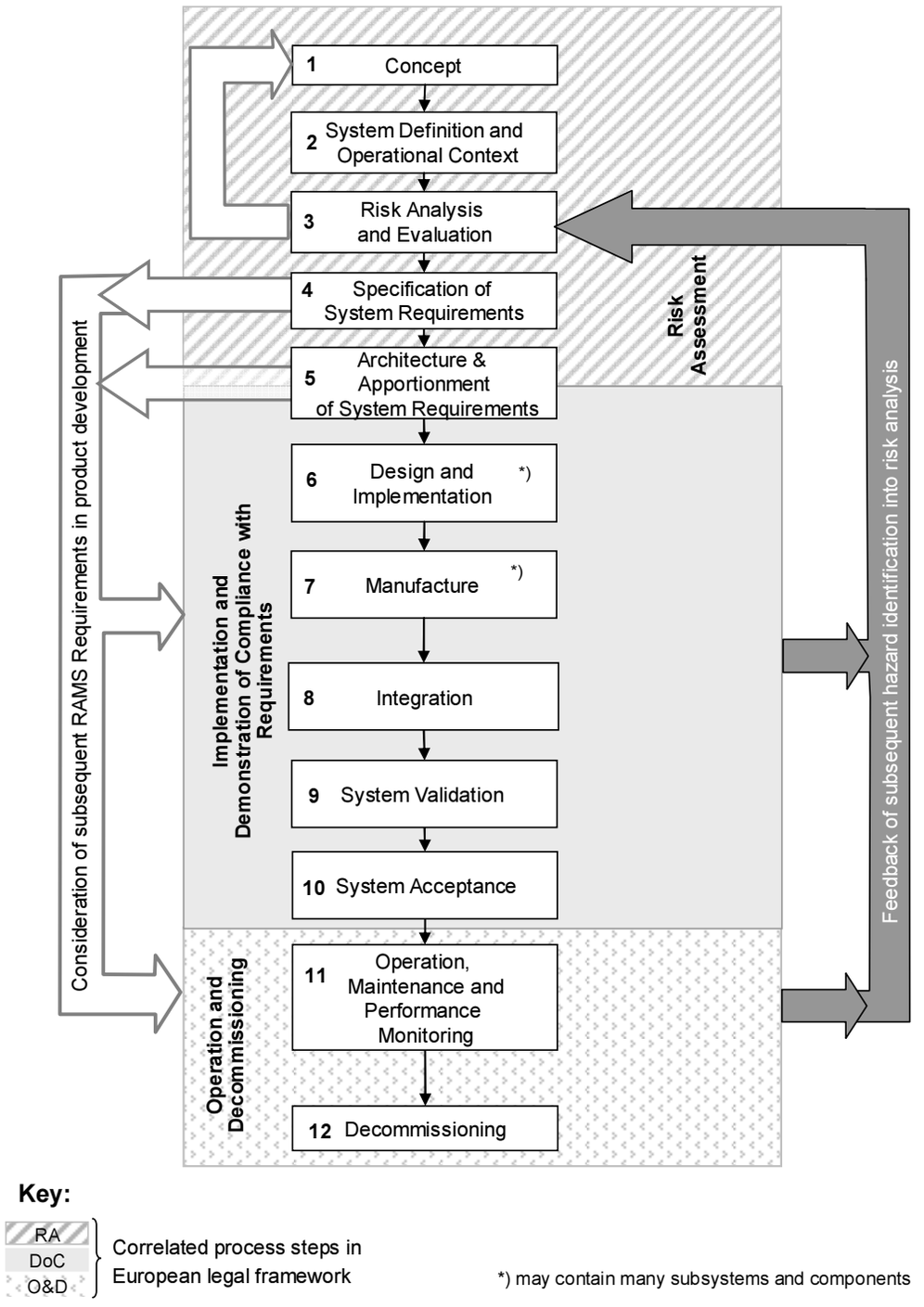

Figure 1. System Safety Life-cycle According to CENELEC Standards

3.1. System Level Perspective

The question of perspective and level is quite fundamental to understanding the system, its constituents, the topology, interfaces and dynamic behaviour. The so-called 'top-level' system perspective is a vision and representation that includes four classes of constituents, namely

a. People comprising users, operators, suppliers and the public (the latter category is relevant to the safety and security issues) that is sometimes referred to as stakeholders,

b. Control and automation system that performs functions based on embedded logic and algorithms in machines of mechanical, electro-mechanical or electronic nature,

c. The infrastructure that supports the functioning of the system. This includes supporting systems and the host environment that surrounds the system including the energy supply, major interfaces with neighbouring or supporting systems/sub-systems, etc.,

d. Processes and rules that govern the interactions between people, automation and the infrastructure. These are a broad range of operational, legal, commercial and emergency response conventions that create a common understanding for all system stakeholders. The socio-economic setting within which a system is realized and operated can also be considered as a part of the environmental rules and constraints that influence the functions and behaviours of the systems.

A general view of the broad system composition is depicted in Figure 2 as the so-called top-level system perspective.

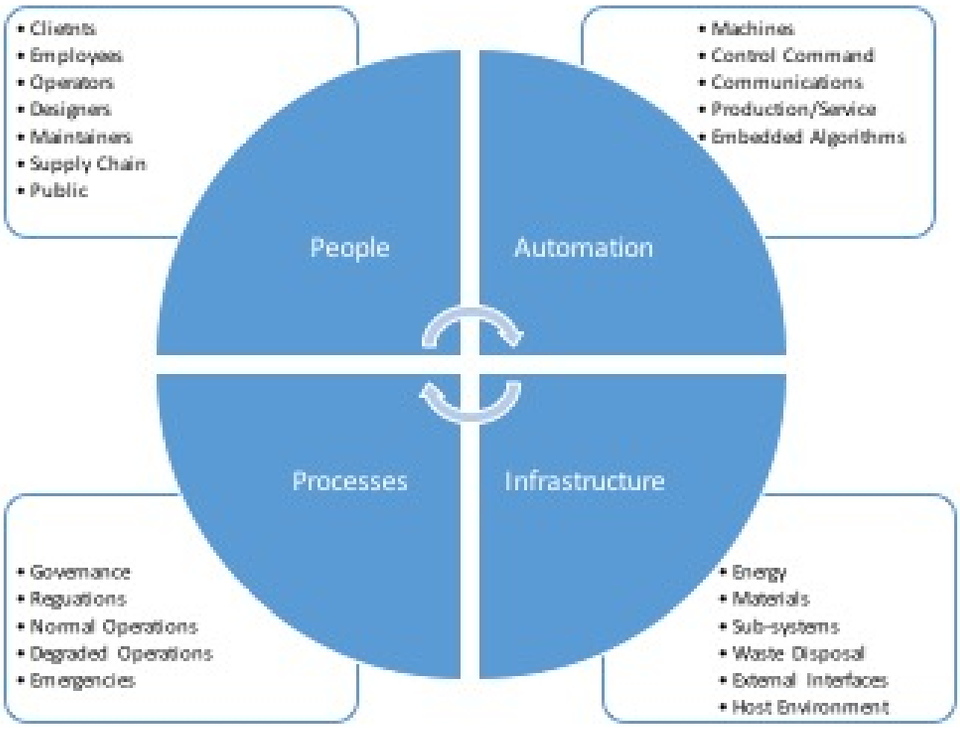

Figure 2. Top-level Railway System Constituents Perspective

The system of interest exists within such a setting and delivers a utility function or service as part of a larger natural or socio-economic system. However, the systematic study and analysis of the most systems requires the forms of conceptualisation, representation and formalisation that provides a backdrop for the study and understanding of the system properties.

http://dx.doi.org/10.5772/62080

Most system studies start with a 'rich-picture' representation that places the system in its host environment and where possible, includes many of the four classes of information detailed above. One such illustration is given in Figure 3 for the safety study of a school within the proximity of a railway environment.

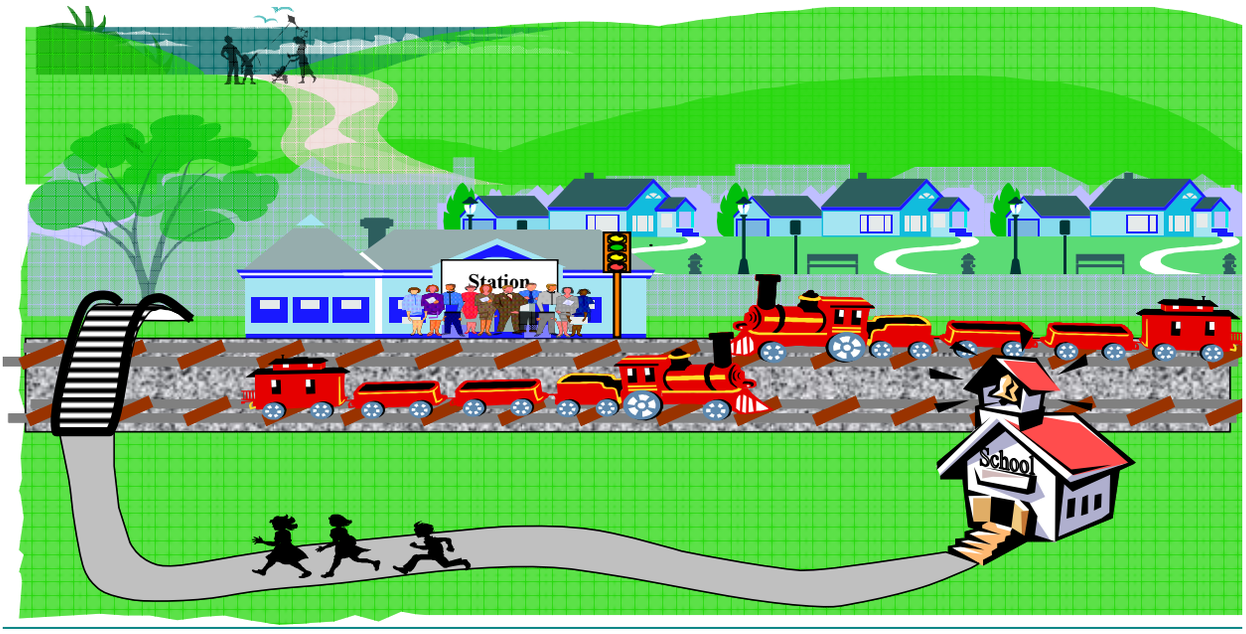

Figure 3. Rich-picture Representation of a Top-level System Perspective

The rich-picture representation and associated often pictorial forms of top-level system representation are largely employed in requirements capture and safety studies at the early phases of the life cycle.

3.2. System Level Requirements

In the life-cycle perspective, especially the one depicted in Figure 1 above, the specification of requirements including the safety requirements commence in phase 4 of the system life cycle. This in practice is unreal and untrue. Most system requirements and indeed some high-level safety requirements are known at the start of the life cycle. These are broadly derived from a number of sources comprising:

1. Past experience of similar or reference systems,
2. Customer and stakeholder expectations,
3. Contractual documents,
4. Operational principles known in the domain and derived or represented in the concept of operation (ConOps),
5. Regulations, standards, rules and codes of practice.

It is worth noting therefore that the system performance requirements are not strictly the matter for a specific time or phase in the life cycle and can predate the system. It is also an evolutionary and iterative process that gains more details the further development moves down the life-cycle phases. The derivation of system level requirements (SLR) is depicted in Figure 4.

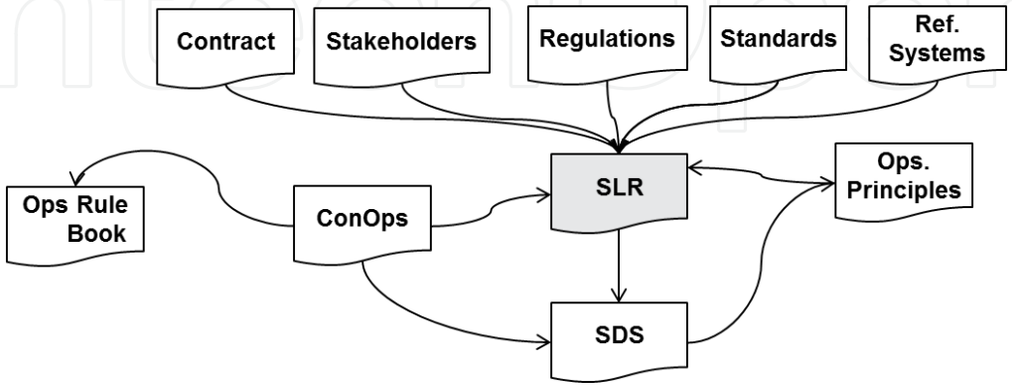

Figure 4. Derivation of System Level Requirements

The feedback loop from later phases of the life cycle such as the system integration phases back to the SLR is quite normal and in the same sense that system safety properties evolve in terms of understanding and detail, requirements, especially at system level may emerge much later than desired. This is a natural consequence of complexity of requirements, expected functions and behaviours as well as the evolving understanding or operational expectations of the client that may impose additional expectations on the system after the early phases of the life cycle.

3.2.1. Classification of SLR

Given the diversity of stakeholders and forms of requirements, it is constructive to classify a large list of requirements into distinct and verifiable classes. These classes are often chosen from performance point of view of stakeholder groupings to make reference and satisfaction arguments simpler and more efficient. The typical classes for such groupings of requirements within a railway context constitute a broad range as depicted in Table 1:

Item	Requirement Class	Scope and Observations
	Technical/functional	Throughput, speed, headway, energy usage, capacity, configurability, size, weight, features, gauge, ...
	Commercial/economic	Costs, finance, social benefit, return on investment,...
	Environmental	Temperature, humidity, vibration, shock, water ingress, rapid cycles, ...
	Integrity	Reliability, availability, maintainability and associated metrics

http://dx.doi.org/10.5772/62080

Item	Requirement Class	Scope and Observations
	Safety	The exposure of people especially clients, operators, service provider and the public to the harmful effects, system failures and accidents, expected level of safety, norms, ...
	Security	Immunity of the system to malicious intent in physical and cyber spaces including surveillance, espionage, attacks, contamination by CBRN,...
	Quality	Relating to system's materials, construction, assembly, installation, ambience, feel, appearance, comfort, ...
	Sustainability	Energy optimization, use of renewables, impact on emissions to the environment, use of rare materials, waste disposal, ...
	Service	Ease of use, alighting & egress, ride quality, HVAC, lighting levels, seating, standing support, passenger density, ...
	Operational	Operational modes, operational principles & rules that have to be observed, trains per hour, door operations, dispatching and station management, degraded operations, emergencies & evacuation, ...
	Usability	Accessibility issues for the elderly and disabled, lifts, support staff, ramps, steps, hand rails, ...
	Social	Scope of service, pricing, user affordability considerations, potential for suicides, ...
	Regulatory	The rules, regulations, targets and standards applicable to the design, development, installation, testing, commissioning and full passenger service, ...
	Temporal	The timing and speed of execution of the project, delivery in staged phases, operational constraints, dwell times, service periods, ...
	Contractual/legal	The obligations of the supply chain in delivering the requirements both legal as well as contractual, penalties and loss limitation, staged payments, operation and maintenance considerations, force majeure conditions, ...
	Performance monitoring	Proactive and reactive monitoring of system performance based on credible systemic predictors/indicators, identification of critical system states, avoidance of down times and accidents through intelligent supervisory systems, ...
	Human resource	The numbers, types and essential knowledge, experience and seniority of the human resources required to operate, monitor and maintain/upgrade the system including resources from the supply chain and temporary staff, organisational structure, reporting, health and safety issues, control and command, necessary licensing, ...

Item	Requirement Class	Scope and Observations
	Training and competencies	The initial training for the different classes of operators, maintainers, support and auxiliary staff to bring them to the minimum level of competence for operational readiness and continued maintenance of the knowledge in the event of system change and upgrades, ...
	Business continuity	Full consideration of maintaining a service level in the event of natural or manmade disasters and major disruptions, redundancy and operational contingencies in such circumstances, ...
	Operational readiness	Consideration of a minimal configuration of the system, supporting sub-systems, human resources, infrastructure, timing, time tabling and response arrangements that render a new system or one recovering from failure or degradation ready for full service operations, ...
	Expected life and life-extension	The client's expectation of the utility and continued functionality of the system in terms of normal operational life, obsolescence, necessary upgrades and maintenance activities and decision criteria for decommissioning and disposal of the system including safety and sustainability considerations, ...
	Special interest	Requests, needs and expectations of various social and formal groups who will be affected by the operation of the system including proximity, noise and vibration levels, EMC, disturbance, working hours, contingencies in the event of major accidents and catastrophes, ...

Table 1. Classification of System Level Requirements for a Railway Context

Any PSP may have an impact or specifically fit within one or more of the above classes. In this spirit and contrary to the immediate focus on a technical system, the classifications depicted in Table 1 should be used as a check-list to capture potential impact of any PSP on wider classes of requirements than mere technical and safety dimensions.

4. System Level Safety and Security Requirements

Safety is a system level emergent property and can best be understood and assured through a systems and high-level perspective. The highest level of perspective for the railways the so-called 'top-level' is the entire railway as a system comprising the constituents detailed in Section 3.1. Understanding of the total railway system safety performance requires a systematic study of the system level interactions between the system constituents and people exposed to the machinery, infrastructure and operations of the railway system. The CENELEC Technical Report TR50451 [3] developed to support EN50129 developed in 1998 details a perspective on the whole railway safety in which three key stakeholders collaborate to understand, analyse and communicate the principal requirements. The principal active stakeholders are

http://dx.doi.org/10.5772/62080

the infrastructure manager (IM) and the railway undertakings (RU) who operate the services. The third key stakeholder involved is the safety regulator, often a government appointed entity. The proposed perspective is for the principal stakeholders who understand the operational railway, that is the RU and IM, to conduct safety analysis, identify system level hazards, conduct risk analysis and determine the tolerability level for the key system level hazards that they manage. This is referred to as the determination of the tolerable hazard rate (THR). The concept is depicted from CENELECTR50451 in Figure 5.

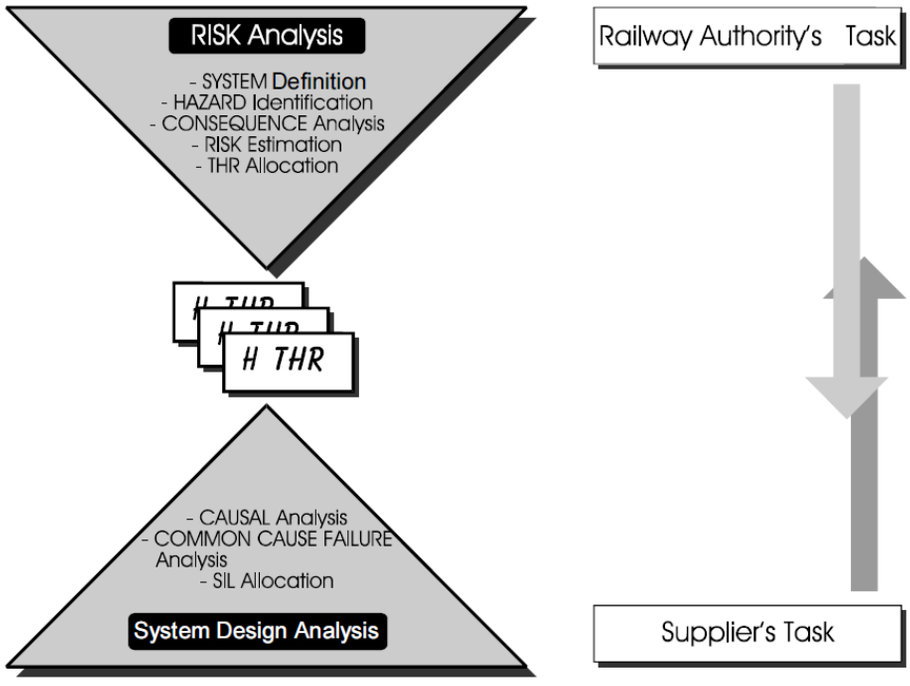

Figure 5. Collaborative Approach to Railway System Safety, Stakeholders and Responsibilities

The tolerable rate for a hazard (THR_H) and the derivation of safety integrity level (SIL) are presented in Figure 5 in the relative order and ownership.

The manufacturers, service providers and supply chain are expected to employ the published THRs to determine what hazards relate to their services/products and determine their share of the hazards affected and SIL applicable to their PSP/service. This is principally a collaborative approach to the achievement of system safety that is likely to render more benefits to the industry than the current disjointed and market driven approach.

4.1. Product Level Safety Requirements Specification

The system safety life cycle as depicted in Section 2 implies that the specification of the system requirements, especially the safety requirements for a PSP commences after system risk analysis, that is in phase 4 and well after the start of a project or programme. Whilst many of the detailed safety requirements emerge from the identification of the product/system behaviours that lead to hazardous states, in a similar manner to the general system require-

ments, many of the safety requirements are known at a high level of detail at the start of a project or programme. These come from a multiplicity of sources, standards, rules, reference products/systems, regulations, customer needs, existing operational safety performance data, existing operational principles, safety functions and finally, any industry level set of safety hazards. This is depicted in Figure 6. These are all recorded in the product/SLR as detailed in Table 1 and the system level safety requirements (SLSR) that constitute a subset.

In principle, if the national level safety data in terms of principal railway hazards and the THRs are known, then these can used together with a causal analysis and apportionment to derive the safety requirements for a complete PSP. Alas, in the absence of such desirable data, the process depicted here is the next best alternative solution to the identification of PSP safety requirements.

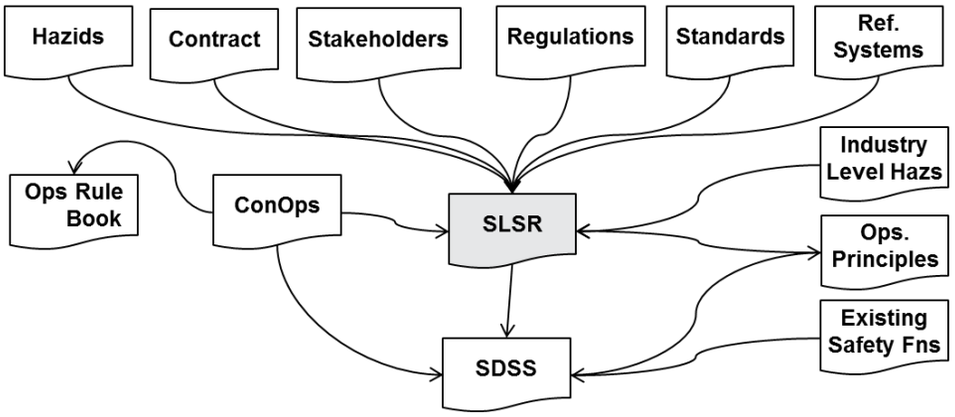

Figure 6. Derivation of System Level Safety Requirements for a PSP

It is also customary to initiate safety activities at the outset of a project or programme through conducting high-level hazard studies. The preliminary hazard studies that lead to an understanding of the potential system hazards are referred to as PHA. These often employ a system representation in the form of rich-picture or Process & Instrumentation Diagram (P&ID) and lead to the identification and capture of hazardous states arising from system composition, placement or the environment since at this stage, not much is known about the total system functionality or design. The PHA is then followed by IHA/OHA/SHA/SSHA at later stages of the life cycle as the design and development, integration and construction progresses.

The relationship between safety studies and the life-cycle phases is depicted in Table 2.

Item	LC Phase	Principal Safety Activity
1	Concept definition	· Hazid of system concept representations · Hazid of system composition, topology, placement, interfaces & Comms · Verify against industry hazards · Verify against ref system hazards

http://dx.doi.org/10.5772/62080

Item	LC Phase	Principal Safety Activity
		· Conduct PHA · Establish hazard log and capture all identified system level hazards
2	Detailed definition and operational context	· Evaluate past experience data for safety · Establish safety plan (overall) · Hazop of Ops Scenarios · Specify system functions and tag the safety related functions · Identify safety protection functions · Conduct SHA and develop core hazards · Conduct IHA &SSHA on the Comms and sub-systems · Hazard log capture
3	Risk analysis and evaluation	· Determine the risk acceptance principles and criteria · Perform system risk analysis based on core hazards · Perform risk evaluation · Determine THRs · Hazard log capture and update
4	Requirements (including Safety Requirements) Specification	· Specify top-level system safety requirements · Define safety acceptance criteria for the system · Define safety-related functional requirements · Determine SIL for safety functions · Establish safety validation plan · Hazard log capture and update
5	Architecture and apportionment	· Apportion system safety targets & requirements · Specify sub-system and component safety requirements · Allocate safety functions to sub-systems · Define sub-system and component safety acceptance criteria · Update safety plan and safety validation plan · Hazard log capture and update
6	Design and implementation	· Implement safety plan by review, analysis, testing and data assessment · Implement safety functions in line with relevant SIL guidelines in reference standards · Ensure hazard control and risk mitigation solutions are designed in · Justify safety-related design decisions · Undertake project control covering: · Safety management · Control of sub-contractors and suppliers · Develop test scripts · Prepare generic product safety case · Hazard log update with all hazard control options implemented
7	Manufacture/production	· Implement safety plan for production activities

Item	LC Phase	Principal Safety Activity
		· Hazard log update
8	System integration	· Verify safety functions and interfaces · Derive safety-related application conditions · Hazard log update
9	Validation	· Implement commissioning programme · Implement validation plan · Conduct Safety Validation tests, analysis · Prepare specific application safety case · Seek safety approvals · Hazard log update with test results, new hazards
10	Acceptance	· Assess specific application safety case · Detail all safety-related application conditions (SRACS) in the O&M Manuals · Close out all hazard-related actions · Ensure operational readiness · Hazard log update and handover
11	Operation and Maintenance& Performance Monitoring	· Undertake on-going safety centred maintenance · Assess the safety impact of any system upgrades and conduct risk analysis before implementation · Perform on going safety performance monitoring and hazard log maintenance · Implement SRACs · Collect, analyse, evaluate and use performance & safety statistics · Capture any emerging hazards in the hazard log
12	Decommissioning	· Establish Decommissioning Safety Plan (DSP) · Perform hazard analysis and risk assessment for decommissioning activities · Implement DSP

Table 2. LC Phase-related Principal Safety Activities

In principle, safety requirements of a composite system comprise functional and non-functional categories. The automation and control systems generally deliver algorithmic safety functions hence largely satisfy functional safety requirements (FSaR) even though any product, system, process/service may additionally have non-functional requirements that affect its safety performance.

The FSaR category is depicted in the class definition in Table 3.

The non-functional category largely relate to operating and environmental conditions, health and safety issues, materials, packaging and manufacturing aspects of a PSP and are not treated in this guidance. The non-functional safety requirements (NFSaR) are depicted in the class definition in Table 4.

Item	Class: Functional Safety Requirements (FSaR)
Attributes	· Is a positive statement of desirable safe performance to be achieved · Relates to ensuring the control or supervision of an undesirable system hazard to be avoided · Relates to a user/environment/operational need · Can be classed as Mandatory or Desirable · All Mandatory FSaRs shall be met by the design · Has a hierarchy from function to HW, SW and PW
Operations	· FSaRs translate into real algorithmic action/activity that has to be performed by SW, HW, PW or System · Has direct control/protection/supervisory role in system · Has varying risk control/protection capability · Has different levels of confidence defined by SIL · Satisfies one or more classes of Stakeholders · Is traceable to system level requirements (SLR and SLSR) · Has to be specified in a specific level of safety attainment to reduce costs of implementation

Table 3. Functional Safety Requirements Class

Item	Class: Non-Functional Safety Requirements
Attributes	Is a positive statement of desirable safety feature, e.g. electrical, EMC immunity etc. Relates to a user/environment/operational need Can be classed as Mandatory or Desirable All Mandatory NFSaRs shall be met
Operations	NFSaRs translate into features that need to be realised Has varying risk control/mitigation capability Satisfies one or more classes of Stakeholders Is traceable to system level requirements (SLR and SLSR) Influences environmental, safety, health and welfare, materials, packaging and manufacturing aspects

Table 4. Non-Functional Safety Requirements Class

It is also important to note that the apparent overlap between various hazard studies from PHA to SHA is matters of perspective and detail. What is identified at PHA is largely very high level and coarse issues akin to core hazard concept developed in the UK system level study and later adopted by ETCS, the European Train Control System. The more detailed hazards identified at the system and sub-system level often fit within these Core Hazard categories hence no repetition of the effort or waste of energies should occur in subsequent hazard studies.

5. System Level Safety Study–UK National Railways

To this date and since the initial publication of the CENELEC TR-50451 [3] initially published as R009-004 in 1999, only one system level study of the whole railway infrastructure and operations has been conducted in the United Kingdom, largely designed and implemented by the author and the supporting team at Railtrack plc in 1996.

The so-called risk profiling of UK Railways attempted to study the whole railway system from the view point of safety risks posed to three key groups, namely:

1. The Passengers,

2. The Workers and Employees,

3. The General Public and the railway Neighbours.

This national level study was scoped at the level of the whole UK national railway system and after three years resulted in identification, verification and publication of three hazard logs relating to the three groups studied and an integrated quantified safety and environmental risk model.

The idea of core hazard was devised to classify and group hazards with similar root, causation or synergy into larger classes and avoid dealing with many tens of detailed issues identified in the course of the national level study. The core hazards and the detailed hazards are the basis of determining the system level safety requirements (SLSR) for the entire railway. However, since the hazards and the requirements are system level properties that are heavily influenced by the national culture, it is not possible or indeed could be misleading to adopt the SLSR safety requirements from another country. In reality, each nation state needs to conduct their own studies to arrive at a current and culture sensitive nature of the safety risks of their national railways to the population.

The risk profiling of Railways project employed a detailed scenario-based scrutiny of the exposure of each group of people to the operational and infrastructure hazards of the national railway. The scenarios were themed around a 'Day in the Life of...' each group and took three years to complete. The hazards identified through the study were verified against a number of sources by a number of independent engineering safety consultancy organisations. After verification and checks for coverage and completeness, the identified hazards were modelled employing a systematic framework comprising causal, consequence and loss evaluation stages [4] in order to establish the risks and strive towards generating a safety risk profile for the national railways. The outcome was the first total railway system level integrated risk model that was capable of being employed to assess the impact of various changes, technologies and innovations on the safety performance of the national level railway or aspects of it. It also generated THRs for all the published groups of hazards for use in the supply chain. This study influenced TR-50451 [3] and the approach to collaboration in railway safety.

In principle, a national level railway Hazard Portfolio for each of the three affected groups, followed by determination of the risk tolerability level for the occurrence of these hazards is

http://dx.doi.org/10.5772/62080

the only systematic approach to understanding system level safety issues and apportioning these products, systems and processes/services in a traceable, realistic and meaningful manner.

5.1. Passengers group

The national level safety study of the passenger group was planned and conducted over a number of workshops with diverse participants from many of the stakeholder groups. A series of pictographics and photos were taken and composed into 'A Day in the Life of a Railway Passenger' that covered most credible scenarios that a typical passenger would interact with the railways. This comprised entering a railway station, using the facilities, going to a platform, boarding a train, travelling, reaching their destination, alighting and eventually leaving the railway premises. The rich-picture representations were employed as the backdrop to a creative Hazop style process to identify all deviations from the normal behaviour that could result in a hazardous state to which a passenger was exposed to.

By the end of the national level workshops, 101 hazards had been identified [5] for the passenger group taking into account variations in age, conditions and luggage handling. The identified hazards were shared with the participants for offline verification and completeness checks. Through a further review, all hazards with common causality or synergy were grouped as a cluster under a core hazard. For the passenger group, each core hazard was tagged with a H for Hazard, P for Passenger and a unique number that represents the relative proximity of the hazard to an accident scenario. The core hazards for the passenger group, relating to the exposure scenarios throughout a railway journey are depicted as follows.

5.1.1. Core Hazard: HP500 – Abnormal or Criminal Behaviour

The HP500 addresses the range of abnormal and criminal behaviours that are known to take place within the railway infrastructure. This does not, however, address abnormal working practices of railway personnel, with the exception of train drivers and senior conductors. This cluster comprises a number of lower level hazards that were identified at the stakeholder workshops, namely

HP425 Irresponsible behaviour

HP426 Destructive behaviour (all forms)

HP427 Crossing line at station

5.1.2. Core Hazard: HP502 – Crowding

The causal model for HP502 represents the range of factors that potentially could cause a crowding situation to arise (e.g. a special event causing an increase in passengers, or an incident causing panic amongst an otherwise manageable number of passengers).

The consequence model for HP502 represents the development of a crowding situation to a level at which injuries or loss of balance (see HP506) could occur. This hazard cluster comprises:

HP502 *Crowding*

5.1.3. Core Hazard: HP503—Loss of Passenger Compartment Integrity During Movement

The scope of this core hazard includes the following:

- Doors opened early on stopping slam shut or CDL trains, potentially resulting in passengers and workers on the train falling out of the train or passengers and workers on the station platform being struck by open doors.
- Slam shut or CDL trains departing with a door open, potentially resulting in passengers and workers on the station platform being struck by the open door or the open door being struck by a passing train.
- Doors opened during train movement, potentially resulting in passengers or workers falling out of the train.
- Doors on the wrong side of the platform unlocked (on trains with sliding or CDL doors) or opened (on trains with slam shut doors), potentially leading to passengers or workers getting off the train on the wrong side, or falling out of the train onto the track. Also included here are incidents where doors which are on the same side of the train as the platform but which are not adjacent to the platform (e.g. when a train is longer than the platform) are unlocked or opened and passenger or worker leaves or falls out of the train.
- Train carriage decoupling during movement, potentially leading to passengers or workers falling off the train.
- Doors failing to open at a station are included within this core hazard in the causal analysis for consistency with earlier work but consequence barriers are not modelled as it is considered that there are no safety implications within the scope of this core hazard associated with doors failing to open. Train doors are barriers to consequence escalation for other core hazards, for example HP507 'Onset of fire/explosion', but failure of train doors to open does not in itself present a hazard. This cluster comprises:

HP503 *Loss of passenger compartment integrity during movement*

5.1.4. Core Hazard: HP504—Passengers in Path of Closing Train Doors

This hazard encompasses 'passenger in path of closing train door' (HP504) and 'worker in path of closing train' (HW503). The scope of this core hazard includes

- Passenger or worker hit by closing door.
- Passenger or worker caught in door of stationary train, potentially leading to the train moving off, dragging the person along the platform.
- Passenger or worker trying to board a moving train, potentially leading to apparel being caught on the door and dragged along the platform or opening the door then falling and being hit by the door or caught up in the door.

The cluster comprises;

HP504HP504 passenger/apparel in path of closing train door

http://dx.doi.org/10.5772/62080

5.1.5. Core Hazard: HP506—Loss of Balance

We have excluded from this core hazard falls to trespassers and falls occurring on level crossings. The scope of passengers has been enlarged to include all persons in a railway station. We also excluded a few falls that were suicide attempts, but included some where there was no clear determination. We have excluded passengers falling as a result of trying to enter or leave the train, while it is still moving. This cluster comprises

HP413 Loss of balance on the ground

HP414 Loss of balance on stairs and escalators

HP415 Loss of balance getting on and off trains

HP416 Loss of balance whilst in a train

5.1.6. Core Hazard: HP509—Inappropriate Separation between Running Railways and Passengers

The HP509 Core Hazard for inappropriate separation between running rail and passengers has been developed to include those situations where the distance between the running rail and people is not sufficient to ensure the safety of passengers.

This core hazard does not include Core Hazard HN501 failure of level crossing to protect the public from passing trains. This model also does not include incidents of inappropriate separation between running rail and passengers resulting from suicide. Finally, this model does not include incidents of inappropriate separation between running rail and people caused by derailment. This cluster comprises:

HP509Inappropriate separation between rail & passengers

5.1.7. Core Hazard: HP510—Inappropriate Separation between Un-insulated Live Conductors and Passengers

The scope of 'Inappropriate separation between un-insulated live conductors and passengers' includes the following:

HP417 Occurrence of DC power arc

HP418 Existence of touch potential

HP419 Inappropriate separation from DC conductor rail

HP420 Structure in contact with live conductor rail

HP421 Inappropriate separation from OHL

HP422 Structure in contact with OHL

HP423 Occurrence of AC power arc

HP424 Inappropriate separation from OHL induced voltage

5.1.8. Core Hazard: HP512—Passenger Protruding Beyond Train Gauge During Movement

Core Hazards HP512, passenger protruding beyond train gauge during movement, have been developed to include all situations in which a person is protruding outside the gauge of a moving train.

The model excludes incidents resulting from suicide or attempted suicide— these are assumed to be covered under HP500 Abnormal or Criminal Behaviour. The cluster comprises

HP512 Passenger protruding beyond train gauge

5.1.9. Core Hazard: HP513—Unsecured Objects at Height

This core hazard falls within the generic grouping of 'Objects Falling from Height' affecting passengers (HP513) which includes the following:

- Objects falling from height within stations (HP513, HP512) as a result of degradation (e.g. falling glass) or maintenance or construction work.
- Objects thrown at trains (HP513, HW512).
- Falling luggage stored at height on trains and falling train furniture (HP513).
- Dropped crane loads (HW512).

The cluster comprises

HP513 Unsecured objects falling from height

5.1.10. Core Hazard: HP515—Inappropriate Separation between Passengers and Moving Vehicle (Other Than Rail Vehicle)

The scope of this core hazard is concerned with inappropriate separation between passengers (HP515) and moving vehicles (not rail vehicles). This encompasses the following:

- Accidents involving road vehicles in collision with pedestrians, other vehicles or structures in the vicinity of stations and work sites (including workers at level crossings in local control mode).
- Accidents involving non-road motorised vehicles, push trolleys and catering trolleys.
- Accidents involving overturned machinery and inadequate control of wheel set movements.

The cluster comprises:

HP515 inappropriate separation between passenger and moving vehicle (non-rail)

5.1.11. Core Hazard: HP516— Handling Heavy Loads

The hazard is defined to assume some error had occurred in handling a heavy load since otherwise the estimated number of incidents would be so high to be meaningless as a hazard. Various scenarios were identified, including strain injuries from carrying and lifting luggage,

http://dx.doi.org/10.5772/62080

luggage falling on to other passengers usually inside trains and cases of luggage falling down escalators and stairs.

The cluster comprises:

HP516 Error in handling heavy load

5.1.12. Core Hazard: HP517—Incompatibility of Train and Structure Gauge

The HP517 (incompatibility of train and structure gauge) have been developed to include those situations where the clearances between trains and infrastructure have been compromised. This hazard includes events where the train or its load extend beyond the specified gauge due to errors in loading, equipment failures or damage; movement errors leading to the train going onto the wrong route; track defects/misalignment; failures or damage leading to civil structures compromising the clearance. This core hazard does not consider events which have resulted in objects on the line (HP511), railway construction/ maintenance works, unsound structures (HP514) or unsecured objects at height (HP513). The cluster comprises

HP517 incompatibility of train and structure gauge

5.1.13. Core Hazard: HP600—Abnormal Deceleration

The risk model for HP600 'Abnormal deceleration' has been developed to strictly model only those instances of a train's slowing sharply when not actually as a part of a derailment or collision scenario. The consequences of the abnormal deceleration part of derailment and collision scenarios are assumed to be included in the loss estimation for those events. The cluster comprises

HP600 Abnormal Deceleration (super-set of HP518 &HW516)

5.1.14. Core Hazard: HP601—Uncontrolled Approach to Buffer

In the causal model, malicious or reckless behaviour on the part of the driver of the relevant train has been assumed to have been included in the data for 'Driver error'. The causal model has been populated using the SMIS database and data from Health and Safety Executive (HSE) reports.

The consequences of this hazard have been taken forward only to the point of the accident's occurring, that beyond is assumed to be calculated by loss modelling. Therefore, the incidence of fire due to buffer-stop collision has not been separately developed in the consequence model. The consequences have been assumed to fall into three bands: collisions at speeds at or below that for which the buffers have been designed; collisions at speeds greater than that for which the buffers have been designed; and collisions with siding buffer-stops. The effects of TPWS and ATP have been ignored, as they were fitted in only a small minority of cases at the time. The consequence model has been populated using expert judgement. The cluster comprises

HP601 Uncontrolled approach to buffer (HP501 &HW501)

5.1.15. Core Hazard: HP602—Loss of Train Guidance (Passenger Trains)

The risk model for HP602 'Loss of train guidance (Passenger Train)' has been developed to strictly model only those instances where a derailment actually occurs. The losses associated with this model include those occurring before the derailment due to abnormal deceleration, if there are any. However, where such deceleration avoids a derailment, the consequences are included in the 'Abnormal Deceleration' model. The cluster comprises

HP602 Loss of train guidance (Passenger Train) (HP412, HW409 &HN402)

5.1.16. Core Hazard: HP603—Loss of Train Guidance (Freight Trains)

The risk model for HP603 'Loss of train guidance (Freight Train)' has been developed to strictly model only those instances where a derailment actually occurs. The losses associated with this model include those occurring before the derailment due to abnormal deceleration, if there are any. However, where such deceleration avoids a derailment, the consequences are included in the 'Abnormal Deceleration' model. The cluster comprises

HP603 Loss of train guidance (Freight Train) (HP411, HW408 &HN401)

5.1.17. Core Hazard: HP604—Objects/Animals on the Line

The risk model for HP604 'Objects/Animals on the line' has been developed to model only the instances of animals or objects being on the running railway and having some effect thereon. There may be many instances of animals entering and leaving the railway having no effect at all and being entirely unnoticed. These scenarios are not modelled, neither are those in which other objects, such as litter, come to rest on the railway, but do not affect the system at all. Instances of objects and animals on the line causing fires are captured in the fire models and not within this model. This model also specifically excludes all causes and consequences arising from the Core Hazard HN501 'Crossing running railway at a Level Crossing'. The cluster comprises

HP604 Object/animals on line (HP511, HW510 &HN514)

5.1.18. Core Hazard: HP605—Inappropriate Separation between Trains

The risk model for HP605 'Inappropriate separation between trains' has been developed to address only the scenarios in which the separation between trains, normally provided by the signalling system, has broken down. This hazard is defined such that there is no interface between it and the 'Loss of Balance' core hazards. The cluster comprises:

HP605 Inappropriate separation between trains (HP505, HW504, HN505)

5.1.19. Core Hazard: HP606—Onset of Fire/Explosion

Core Hazard HP507 onset of fire/explosion for passengers has been developed to include those situations where fire is a spontaneous event, however, the situations where fire is a secondary

http://dx.doi.org/10.5772/62080

consequence of a train collision or derailment are excluded. Noxious fumes are included when the cause is fire related.

Consideration has been given to the interface of his Core Hazard with Core Hazard HP500 / HW500 / HN500 abnormal or criminal behaviour. The cluster comprises:

HN400 Fire at line side

HP400 Fire inside passenger carriage

HP401 fire outside passenger electric train

HP402 fire outside diesel passenger train

HP403 Fire at station

HW400 fire on electric freight train

HW401 fire on diesel freight train

5.1.20. Core Hazard: HP607—Unsound/Unsecured Structures

The HP514 Core Hazard for Unsound/Unsecured Structure has been developed to include those situations where structures are unstable creating a threat to passengers or neighbours. This core hazard shall not include instability of trains or the movement of materials on trains. Consideration has been given to the interface of this core hazard with the core hazards object on line and inappropriate separation between trains.

All structures going beyond the railway boundary are covered here and not in HP509, inappropriate separation between running rail and passenger.

Neither the causal nor the consequence models refer to situations where structures are unstable creating a threat to workers. This is a part of Core Hazard HW512 Unsecured Objects at Height and Core Hazard HW517 Collapsing Machinery/Materials/ Structures. The cluster comprises

HP404 Unsound/Unsecured Tree

HP405 Unsound/Unsecured Tunnel

HP406 Unsound/Unsecured Under-bridge / Culvert

HP407 Unsound/Unsecured over-bridge

HP408 Unsound/Unsecured Station

HP409 Unsound/Unsecured Signalling Structure

HP410 Unsound/Unsecured Electrification Structure

5.2. Workers Group

The national level safety study of the railway workers group was planned and conducted over a number of workshops with diverse participants from many of the stakeholder groups. A

similar set of prompts and photos focused on this group were taken and composed into 'A Day in the Life of a Railway Worker' that covered most credible scenarios that employees/workers interact with the railways. This comprised planning, operating, station duties, maintenance and driving of trains. The pictorial scenarios were likewise employed as the backdrop to a creative Hazop style process to identify all circumstances where railway employees/workers were potentially exposed to hazardous states.

By the end of the national level workshops, 119 hazards had been identified [5] for the workers group. Through a further review, all hazards with common causality or synergy were grouped as a cluster under a core hazard. For the passenger group, each core hazard was tagged with a H for hazard, W for workers and a unique number that represents the relative proximity of the hazard to an accident scenario. The core hazards for the workers group, relating to the exposure scenarios are depicted as follows.

5.2.1. Core Hazard: HW500—Abnormal or Criminal Behaviour

The model developed for HW500 addresses the range of abnormal and criminal behaviours that are known to be performed within the railway infrastructure. They do not, however, address abnormal working practices of railway personnel, with the exception of train drivers and senior conductors. This was agreed with the experts at the start of the modelling process. The cluster comprises

HW426 Irresponsible behaviour

HW427 Destructive behaviour

HW428 Crossing line at station

5.2.2. Core Hazard: HW502—Loss of Passenger Compartment Integrity During Movement

The scope of this core hazard includes the following:

- Doors opened early on stopping slam shut or CDL trains, potentially resulting in workers on the train falling out of the train or workers on the station platform being struck by open doors.
- Slam shut or CDL trains departing with a door open, potentially resulting in workers on the station platform being struck by the open door or the open door being struck by a passing train.
- Doors opened during train movement, potentially resulting in workers falling out of the train.
- Doors on the wrong side of the platform unlocked (on trains with sliding or CDL doors) or opened (on trains with slam shut doors), potentially leading to workers getting off the train on the wrong side, or falling out of the train onto the track. Also included here are incidents where doors which are on the same side of the train as the platform but which are not adjacent to the platform (e.g. when a train is longer than the platform) are unlocked or opened and passenger or worker leaves or falls out of the train.

- Train carriage decoupling during movement, potentially leading to workers falling off the train.
- Doors failing to open at a station are included within this core hazard in the causal analysis for consistency with earlier work but consequence barriers are not modelled as it is considered that there are no safety implications within the scope of this core hazard associated with doors failing to open. Train doors are barriers to consequence escalation for other core hazards, for example HP507 'Onset of fire/explosion', but failure of train doors to open does not in itself present a hazard.

The cluster comprises

HW502 Loss of passenger compartment integrity during movement

5.2.3. Core Hazard: HW503—Worker in Path of Closing Train Doors

This hazard encompasses workers in path of closing train (HW503). The scope of this core hazard includes

- Worker hit by closing door.
- Worker caught in door of stationary train, potentially leading to the train moving off, dragging the person along the platform.
- Worker trying to board a moving train, potentially leading to apparel being caught on the door and dragged along the platform or opening the door then falling and being hit by the door or caught up in the door.

The cluster comprises

HW503 HW503 worker/apparel in path of closing train door

5.2.4. Core Hazard: HW505—Loss of Balance

We have excluded from this core hazard any falls occurring on level crossings, although works crossings were included. There is some overlap at the consequence side with HW508. We have included falls getting on and off trains by drivers and cleaning staff who often have to negotiate steps and gaps which would not be encountered by passengers. The cluster comprises

HW410 Loss of balance on the ground

HW411 Loss of balance on stairs and escalators

HW412 Loss of balance getting on and off trains

HW413 Loss of balance whilst in a train

HW414 Loss of balance when working at height

5.2.5. Core Hazard: HW508—Inappropriate Separation between Running Railways and Workers

The HW508 Core Hazard for inappropriate separation between running rail and workers has been developed to include those situations where the distance between the running rail and people is not sufficient to ensure the safety of workers.

This core hazard does not include Core Hazard HN501 failure of level crossing to protect the public from passing trains. This model also does not include incidents of inappropriate separation between running rail and workers resulting from suicides. Finally, this model does not include incidents of inappropriate separation between running rail and people caused by derailment. The cluster comprises

HW402 Red zone working

HW403 Green zone working

5.2.6. Core Hazard: HW509—Inappropriate Separation between Un-insulated Live Conductors and Workers

The scope of 'Inappropriate separation between un-insulated live conductors and workers' includes the following:

HW415 Occurrence of DC power arc

HW416 Existence of touch potential

HW417 Structure exposed to leakage current [DC]

HW418 Inappropriate separation from conductor rail

HW419 Structure in contact with live conductor rail

HW420 Inappropriate separation from OHL

HW421 Structure in contact with live OHL

HW422 Inappropriate separation from OHL induced voltage

HW423 Inappropriate separation from ground potential

HW424 Occurrence of AC power arc

HW425 Structure exposed to current leakage [AC]

5.2.7. Core Hazard: HW511—Worker Protruding Beyond Train Gauge During Movement

Core Hazard HW511, worker protruding beyond train gauge during movement, have been developed to include all situations in which a person is protruding outside the gauge of a moving train.

The model developed excludes incidents resulting from suicide or attempted suicide—these are assumed to be covered under HHW500 abnormal or criminal behaviour. The cluster comprises

HW511 Worker protruding beyond train gauge

http://dx.doi.org/10.5772/62080

5.2.8. Core Hazard: HW512—Unsecured Objects at Height

This core hazard falls within the generic grouping of 'Objects Falling from Height' affecting workers (HW512) that includes the following:

- Objects falling from height within stations (HP513, HP512) as a result of degradation (e.g. falling glass) or maintenance or construction work.
- Objects thrown at trains (HP513, HW512) or hung in front of trains (HW512).
- Falling luggage stored at height on trains and falling train furniture (HP513, HW512).
- Dropped crane loads (HW512).
- Falling objects from the infrastructure (HW512, HN512).

The cluster comprises:

HW512 Unsecured objects at height

5.2.9. Core Hazard: HW513—Inappropriate Separation between Workers and Moving Vehicle (Other Than Rail Vehicle)

The scope of this core hazard is concerned with inappropriate separation between the workers (HW513) and moving vehicles (not rail vehicles). This encompasses the following:

- Accidents involving road vehicles in collision with pedestrians, other vehicles or structures in the vicinity of stations and work sites (including workers at level crossings in local control mode).
- Accidents involving non-road motorised vehicles, push trolleys and catering trolleys.
- Accidents involving overturned machinery and inadequate control of wheel set movements.

The cluster comprises:

HW513 inappropriate separation between workers and vehicles

5.2.10. Core Hazard: HW514—Handling Heavy Loads

The core hazard was defined to assume some error had occurred in handling a heavy load since otherwise the estimated number of incidents could be so high to be meaningless as a hazard. We scoped the hazard to cover manual handling of loads, including unloading from vehicles.

We did not formulate a definition of a heavy load as a specific weight but considered any incident where the handling of a load caused some loss and where the weight of the load was a factor. We followed the general approach of HP516 of dividing the hazard into problems with lifting, carrying or stacking a load. The cluster comprises

HW514 Improper manual handling of heavy load

5.2.11. Core Hazard: HW517—Unsound/Unsecured Machinery/Materials or Structures

The scope of this core hazard includes the following:

- Crane and rail crane collapse potentially leading to a worker being crushed.
- Collapse of stacked materials potentially leading to a worker being crushed.
- Inadequate protection for working at height potentially leading to a worker falling whilst working at height.
- Misuse or inadequate maintenance of tools causing worker injury.

The cluster comprises

HW517 unsound/unsecured machinery/materials/structures

5.2.12. Core Hazard: HW518—Work in Confined Spaces

We kept the scope of this hazard quite large to include events where workers are in spaces such as offices and drivers in cabs and are exposed to hazards such as fumes from batteries. There is probably some overlap with core hazard area HW512 in the consequences relating to workers in a confined space being affected by toxic or hazardous fumes. We have excluded shunting incidents since these are being dealt with under Core Hazard area HW508.

The cluster comprises:

HW518 Work taking place in confined space

5.2.13. Core Hazard: HW519—Contaminated Water and/or Land

The core hazards for contaminated water and/or land for workers and neighbourhood (HW519 and HN502, respectively) have been defined as the release of harmful substances likely to cause contamination of the environment. This allows the consideration of detection, mitigation and remediation barriers in the consequence domain. The release of toxic gases likely to cause harm to workers or neighbours has also been considered under this core hazard.

This core hazard considers harm to workers or neighbours as a result of coming into contact with land, water or air contaminated with harmful substances, rather than coming into contact with the harmful substances themselves although the toxicology is similar, the frequency and dispersion will differ. Core Hazard HW521, workers in proximity to harmful substances covers the case where water or land contamination is not an issue.

The cluster comprises:

HW519 Release of hazardous substances

5.2.14. Core Hazard: HW520—Inappropriate Working Methods/Environment

The scope of this hazard was defined to include most 'occupational' accidents where typically a single worker is affected. We also included the case of crane loads and other mechanical

http://dx.doi.org/10.5772/62080

equipment fouling trains passing nearby as this was always due to operator error. Any particular scenario where an inappropriate working method was applied to result in an incident which was also covered by another core hazard was excluded. For example, if an inappropriate lifting technique was applied to a task involving a heavy object, we did not consider this part of this core hazard but dealt with it under HW514.

The cluster comprises

HW520 Inappropriate working methods/environment

5.2.15. Core Hazard: HW521—Workers in Proximity to Harmful Substances

The Core Hazards Workers in Proximity to Harmful Substances (HW521) have been defined as the hazard presented to workers when in proximity to uncontrolled harmful substances. This includes those harmful substances carried by the railway (dangerous goods) as well as harmful substances routinely used in the running and maintenance of the railway (fuel oils, caustics, etc.). It does not include substances which are harmful only due to their physical state, for example boiling water or hot food, or indeed, railway food in general.

The case where workers come into proximity to harmful substances through contaminated water or land is not considered in this report as that case is covered under Core Hazard HW519 contaminated water and/or land. The cluster comprises

HW521 Workers in proximity to harmful substances

5.2.16. Core Hazard: HW522—Road Vehicle Accidents

Core Hazard HW522, road vehicle accidents covers accidents to workers in road vehicles whilst on railway business, but on the public highway. The model excludes incidents on Railtrack property and controlled infrastructure—these are covered under Core Hazards HW513/HP515 inappropriate separation between workers/passengers and Moving Vehicle (other than Rail Vehicle).The cluster comprises:

HW522 Road Vehicle Accident

5.2.17. Core Hazard: HW523—Objects Thrown or Falling from Train

The core hazard considered in this report considers the impact on workers of 'Objects Thrown or Falling from Train'. The impact on neighbours of objects thrown or falling from trains is included in the work scope for HN511 and is not included in the scope of work reported here. The work scope for HW523 includes the following:

- Objects deliberately thrown from trains.
- Objects falling off trains, for example shattered brake disk.
- Loads falling from freight trains, including ballast.

The cluster comprises:

HW523 Object thrown or falls from train

5.3. Neighbours group

The national level safety study of the railway neighbours group was planned and conducted over a number of workshops with diverse participants from many of the stakeholder groups. Neighbours are those who live within proximity of the railway environment and cross the line at level crossings. A similar set of prompts and photos focused on this group were taken and composed into 'A Day in the Life of a Railway Neighbour' that covered most credible scenarios that neighbours of the railways get exposed to generally involuntarily. The pictorial scenarios were employed as the backdrop to a creative Hazop style process to identify all circumstances where railway neighbours were potentially exposed to hazardous states.

By the end of the national level workshops, 64 hazards had been identified [5] for the neighbours group. In a similar manner, Core Hazards were developed for the neighbour group; each Core Hazard was tagged with a H for Hazard, N for Neighbour and a unique number that represents the relative proximity of the hazard to an accident scenario. The core hazards for the neighbour group, relating to the exposure scenarios are depicted as follows.

5.3.1. Core Hazard: HN500—Abnormal or Criminal Behaviour

The models for HP500, HW500 and HN500 address the range of abnormal and criminal behaviours that are known to be performed within the railway infrastructure. They do not, however, address abnormal working practices of railway personnel, with the exception of train drivers and senior conductors. This was agreed between Human Engineering and Railtrack at the start of the modelling process. The cluster comprises

HN416 Suicide attempt

HN417 Trespass

HN418 Abnormal behaviour at special events

5.3.2. Core Hazard: HN501—Crossing Running Railway at Level Crossing

Core Hazard HN501, crossing running railway at a level crossing, has been developed to include all situations in which a user (i.e. a Neighbour) is present on a level crossing without the intended degree of protection from trains. This may arise from intentional or inadvertent misuse of the crossing by the neighbour as well as from failures and errors in railway equipment and procedures.

The definition excludes situations in which harm may arise when using a level crossing as intended, for example if a user falls and injures themselves on a crossing but is still able to cross within the design time limit. Such occurrences are assumed to be subsumed within Core Hazard HN506, loss of balance.

The model excludes incidents at level crossings resulting from suicide or attempted suicide—these are assumed to be covered under HN500 abnormal or criminal behaviour

The model is limited to neighbour hazards and thus does not consider hazards at worker crossings provided within stations, depots, sidings etc. Un-authorised neighbour use of such

http://dx.doi.org/10.5772/62080

crossings should be regarded as abnormal or criminal behaviour (HN500), being a form of trespass. (Unauthorised passenger use is covered in Core Hazards HP509 inappropriate separation between running railway and workers/ passengers.)

It should be noted that HN509, inappropriate separation between running railway and neighbourhood, did not consider level crossing hazards. HN501 and HN509 are thus taken to be mutually exclusive.). The cluster comprises

HN480 crossing running railway at a manual level crossing

HN481 crossing running railway at an automatic level crossing

HN482 crossing running railway at user worked level crossing

HN484 crossing running railway at a level crossing

5.3.3. Core Hazard: HN502—Contaminated Water and/or Land

The core hazards for contaminated water and/or land for neighbours have been defined as the release of harmful substances likely to cause contamination of the environment. This allows the consideration of detection, mitigation and remediation barriers in the consequence domain. The release of toxic gases likely to cause harm to workers or neighbours has also been considered under this core hazard.

This core hazard considers harm to workers or neighbours as a result of coming into contact with land, water or air contaminated with harmful substances, rather than coming into contact with the harmful substances themselves—although the toxicology is similar, the frequency and dispersion will differ. The cluster comprises

HN502 Contaminated Water and/or Land

5.3.4. Core Hazard: HN503—Electro-Magnetic Interference (EMI) Caused to by Railway Operations

EMI caused by railway operations to businesses, general public, adjacent buildings, hospitals, HN503 has been developed to include those situations where EMI from the infrastructure or rolling stock could affect the safety of neighbours directly. This core hazard does not include EMI caused by infrastructure or rolling stock to signalling and track circuits, or interference between the rolling stock and infrastructure. Such interference could be considered part of the base event frequencies for other core hazards. Interference caused by radio systems is not explicitly examined, it is considered to be subsumed into the frequencies of the initiating events identified and would be subject to the same design controls and regulations. In addition, this core hazard does not consider the effects of earth leakage currents causing corrosion of steel pipelines or structures. Thus issues such as HN30 (corrosion of structures from dc rail systems) are covered under HN510. That core hazard also covers the possibility of electrocution due to inductive pickup in cables running adjacent to the AC electrified lines. The cluster comprises

HN503 EMI impact on neighbourhood

5.3.5. Core Hazard: HN504—Impact from Railway Construction/Maintenance Works

The scope of 'impact from railway construction and maintenance works' includes the following:

- Inappropriate construction and maintenance practices' not included under other core hazards
- Dumping heavy loads onto roads, buildings and property of neighbours

Release of flammable materials (other than gas mains) and damage to electrical cabling and gas mains

The cluster comprises

HN504 Impact from railway construction/maintenance works

5.3.6. Core Hazard: HN506—Loss of Balance

We have excluded from this core hazard falls to trespassers and falls occurring on level crossings. As all persons on stations are regarded as passengers for the purpose of this project, the relevant neighbours for this core hazard are basically those persons using footpaths and footbridges which form part of the railway infrastructure. Footpaths alongside public roads are part of the public highway and are excluded. The cluster comprises

HN403 Loss of balance on the ground

HN404 Loss of balance on stairs

5.3.7. Core Hazard: HN509—Inappropriate Separation between Running Railway and Neighbourhood

The HN509 Core Hazard for inappropriate separation between running rail and neighbours have been developed to include those situations where the distance between the running rail and people is not sufficient to ensure the safety of passengers, workers or neighbourhood.

This core hazard does not include Core Hazard HN501 failure of level crossing to protect the public from passing trains. This model also does not include incidents of inappropriate separation between running rail and neighbourhood resulting from suicide. Finally, this model does not include incidents of inappropriate separation between running rail and people caused by Derailment. The cluster comprises

HN509 Inappropriate separation between rail &neighbours

5.3.8. Core Hazard: HN510—Inappropriate Separation between Un-insulated Live Conductors and the Public

The scope of 'inappropriate separation between un-insulated live conductors and the public' includes the following:

HN405 Occurrence of DC power arc

http://dx.doi.org/10.5772/62080

HN406 Existence of touch potential

HN407 Structure exposed to leakage current [DC]

HN408 Inappropriate separation from DC conductor rail

HN409 Structure in contact with live conductor rail

HN410 Inappropriate separation from OHL live conductor

HN411 Structure in contact with live OHL

HN412 Inappropriate separation from OHL induced voltage

HN413 Inappropriate separation from ground potential

HN414 Occurrence of AC power arc

HN415 Structure exposed to leakage current [AC]

5.3.9. Core Hazard: HN511—Flying Debris from Moving Train and Objects Falling from Trains

HN511 Core Hazard for flying debris from moving trains and objects falling from trains has been developed to include those situations where parts of the train and objects carried on the train are separated from the moving train and are a potential hazard to neighbours.

This core hazard does not include things falling from bridges into the surrounding neighbourhood. These incidents are covered in the Core Hazard HN512 unsecured objects at height.

Neither the causal nor the consequence models refer to situations where parts of the train and objects carried on the train are separated from the moving train and are a potential hazard to passengers or workers. The cluster comprises

HN511 Flying debris / objects falling from trains

5.3.10. Core Hazard: HN512—Unsecured Objects at Height

This core hazard falls within the generic grouping of 'Objects Falling from Height' affecting neighbours (HN512) which includes the following:

- Objects falling from height within stations (HP513, HP512) as a result of degradation (e.g. falling glass) or maintenance or construction work.
- Objects thrown at trains (HP513, HW512) or hung in front of trains (HW512).
- Falling luggage stored at height on trains and falling train furniture (HP513, HW512).
- Dropped crane loads (HW512).

Falling objects from the infrastructure (HW512, HN512).

The cluster comprises

HN512 Unsecured objects falling from height

6. System Level Security Issues

The transportation network constitutes the artery of economic activity and growth in modern economies. Whilst challenged by telecommunications and internet technologies, the movement of goods and people is still an indispensable aspect of social and economic life contributing around one tenth of the GDP in the developed world[1]. It is not surprising therefore to find transportation on the social and political agenda and any faults, failures and consequent accident, being given a high degree of publicity and exposure. Traditionally, the key mantra in transportation has been safety followed by reliability, punctuality, cost, journey time and quality of travel. This has held true so far for the most modes of transport until recently when malicious intent with the aim of disrupting the network, victimising its customers and inflicting large economic losses has added a new ingredient to the traditional concerns of the industry. The malicious intent broadly falls into the following categories:

- Antisocial Behaviour and Vandalism
- IP Espionage/Violations
- Theft, Extortion, and Fraud
- Robberies, Assaults
- Sabotage
- Terrorism and CBRN Attacks

Whilst vandalism is of limited consequence and often related to adventure seeking youth, the other categories of concern specifically terrorism pose a largely new sinister development often beyond the powers of transportation authorities to predict, prevent or contain. This is where the power of scientific structured approaches and methodologies principally applied in safety engineering can be exploited to render assurance in transportation security in road, rail, shipping and aviation transport hubs.

The proficient assessment, control and mitigation of safety and security risks demand a systematic and objective approach to understanding and proactive management of response processes. However, the traditional focus of security relating to the physical infrastructure and systems is now extended to cyber systems in view of the extensive deployment of modern communications and computing in the railways. A systematic approach to system level security should consider physical and cyber threats and vulnerabilities to assure adequate security throughout the life cycle of the product, process, system or undertaking.

Many facets of a system's performance are inter-related and overall optimisation requires a reasonable insight into the desirable system properties and performance profile. This is equally applicable to the transportation and railways where the provision of service is nowadays taking place within a commercial and cost/performance conscious environment.

1 U.S. Department of Commerce, Bureau of Economic Analysis

http://dx.doi.org/10.5772/62080

Adoption of a systemic and numerate approach to safety and security assurance within an integrated systems framework yields a more inclusive understanding of key facets of performance and the inevitable trade-offs between cost, reliability, quality, safety, security and capacity, journey time/punctuality in the railway context. It also generates rational criteria in support of decision making thus reducing the dependency upon opinion-based subjectivity, lengthy processes and less-informed costly choices. The enhanced objectivity and transparency would result in streamlined decision making and more efficient/responsive processes thus saving time and cost and fostering progress. Additionally, it generates major economic benefits by arriving at a right solution first time. In short, a more objective and numerate approach could help to avoid the subjectivity which be-devils much of the current approach to safety and security management.

Finally, an integrated approach to safety and security assurance that is based on a generic accident model is intuitively more pertinent than one based on anecdotal observation and view of available technologies. It rebalances focus on risks that arise during design, installation, operation, maintenance and retrofitting. It cuts across organisational boundaries, roles, responsibilities and requisite competences that, in the system life-cycle approach, tend to be overlooked thus constraining our perception of risks.

In view of the increasing concerns over security of the transportation systems, the advanced processes and methodologies principally developed and applied in safety critical industries such as nuclear, transportation, oil and gas industries should be extended to the prognosis of transportation vulnerabilities to malicious intent[2]. The new framework is intended to principally harness the significant overlaps between safety and security landscape to offer:

- Systematic and scientific study of transportation networks with a view to identify vulnerabilities to malicious intent in a multi-modal environment whilst also identifying safety and environmental issues.
- Assessment of the risks associated with significant hazards, vulnerabilities or threats.
- Identification of principal elimination, control and mitigation measures.
- Cost-benefit studies to provide technical, procedural and organisational risk elimination/control/mitigation measures with highest potential impact.
- Transportation threat/vulnerability log to keep key stakeholders informed and engaged in the overall assurance process.
- Transportation surety cases to capture the system, safety and security issues (hazards, threats and vulnerabilities), control and mitigation measures and the rationale for the continued vigilance and continual improvement.
- Safety and security (Surety) management systems to provide a framework for continued control and fulfilment of the obligations by the duty holders.

2 UITP-UIC Press Release June 2004

The key benefits will accrue from a structured and cost-effective and high-performance approach to the integrated safety and security assurance of products, systems and services hence surety. In view of the generic nature of the process, these capabilities can be extended to provide the integrated services beyond transportation.

Integrated framework for assurance of safety and security is highly pertinent to the emerging profile of the railways in that, whilst safety is subject to an impressive record of improvement, security is a largely unknown and poses the bigger challenge in the overall assurance landscape.

The risk profiling of the national railways depicted in Section 5 did not take security threats and system level vulnerabilities into account. This was largely driven by the concerns over network safety at the time and lack of immediate security threats to the railways. Ever-since, railways and mass transit systems in the European mainland and indeed in Asia have been targets of attacks and terrorism highlighting the need for a consistent, comprehensive and effective approach to security assurance alongside that of safety.

7. Safety Roles and Competences

The safety performance of the various transportation modes is on the steady improvement largely driven by better regulation, improved deployment of communications and computing technologies in spite of rising speeds and passenger numbers. Many countries in North West Europe outperform the European average for passenger and workforce fatalities with Denmark, United Kingdom and Netherlands in the top three best performing countries that have performance an order of magnitude below the European average.

The European Railway Agency (ERA) has published indicative statistics on the relative safety of various transportation modes that indicates railways are approaching aviation levels of safety on a normalised (per billion kilometre of passenger travel) basis (Table 5).

Transport mode	Fatality risk (2008–2010) Fatalities/billion passenger kilometres
Airline passenger	0.101
Bus/coach occupant	0.433
Car occupant	4.45
Powered two-wheelers	52.593
Railway passenger	0.156

Table 5. Relative Safety of Transportation Modes (Source ERA)

Taking the top level system's constituents perspective as depicted in Figure 2, we postulate that whilst advancing technology has made significant contributions to the reliability and

integrity of the automation and infrastructure, the human (people and process) aspects have lagged behind in the relative scale of improvement. The principal aspects relating to people's influence on the safety performance relate to their competence and the collective values/behaviours referred to as safety culture. The rules, codes of practice and standards constitute the other key contributory facet of overall system safety framework. The desired improvements in rules and standards as well as understanding and improving collective safety culture are beyond the scope of the current discussion. Here, we concentrate on the systematic characterisation, evaluation, assessment and management of safety competences as a key aspect of the human dimension in safety performance.

7.1. Competence

The European Guide to good practice in knowledge management [6] defines competence as an appropriate blend of knowledge, experience and motivational factors that enables a person to perform a task successfully. In this context, competence is the ability to perform a task correctly, efficiently and consistently to a high quality, under varying conditions, to the satisfaction of the end client. This is a much more demanding portfolio of talents and capabilities than successful application of knowledge. So a competent person is much more than and knowledge worker [20]. Competency may also be attributed to a group or a team when a task is performed by more than one person in view of the multi-disciplinary nature, complexity or the scale. A competent person or team requires a number of requisite qualities and capabilities, namely

1. The domain knowledge empirical, scientific or a blend of both.
2. The experience of application (knowing what works) in different contexts and the requisite skills.
3. The drive, motivation to achieve the goals and strive for betterment/excellence as well as appropriate behaviours such as team work, leadership, compliance with professional codes etc.
4. The ability to adapt to changing circumstances and demands by creating new know-how.
5. The ability to perform the requisite tasks efficiently and minimise wastage of physical and virtual resources.
6. The ability to sense what is desired and consistently delivers a high quality to the satisfaction of the end client(s).

The right blend of these abilities renders a person or group of people (a team) competent in that they would achieve the desired outcomes consistently, efficiently, every time or more often than not satisfying or exceeding the expectations of the clients over varying circumstances. Such persons/groups will be recognised for their mastery of the discipline and not just considered a fount of relevant knowledge often characterised by qualifications. In this spirit, competence is the ability to generate success, satisfaction, value and excellence from the application of knowledge and knowhow.

The Business Dictionary [7] defines competence as a cluster of related abilities, commitments, knowledge and skills that enable a person (or an organisation) to act effectively in a job or situation. It further states that competence indicates sufficiency of knowledge and skills that enable someone to act in a wide variety of situations. Because each level of responsibility has its own requirements, competence can occur in any period of a person's life or at any stage of his or her career. With reference to the legal profession, the dictionary defines competence as the capacity of a person to understand a situation and to act reasonably. The disputes regarding the competence of an individual are settled by a judge and not by a professional (such as a doctor or a psychiatrist) although the judge may seek expert opinion before delivering at a judgment.

In the context of UK's Managing Health and Safety in Construction (CDM Regulations), [8] the HSE elaborates on the necessity for competence as follows.

To be competent an organisation or individual must have:

- Sufficient knowledge of the tasks to be undertaken and the risks involved.
- The experience and ability to carry out their duties in relation to the project, to recognise their limitations and take appropriate action to prevent harm to those carrying out construction work, or those affected by the work.

The HSE [9] further maintain that competence develops over time. Individuals develop their competence through a mix of initial training, on-the-job learning, instruction, assessment and formal qualification. In the early stages of training and experience, individuals should be closely supervised. As competence develops, the need for direct supervision should be reduced. If you are engaging a person or organisation to carry out construction work for you, then you need to make a reasonable judgement of their competence based on evidence. The evidence will usually be supplied to you by the person or organisation quoting or bidding for the work. There are many industry card schemes which can help in judging competence. However, the possession of a card by an individual is only one indication of competence. You are expected to make efforts to establish what qualifications and experience the cardholder has.

7.2. Recent Developments

The matters of competence and relevance of the deployed human resource to the requirements of mission and safety critical tasks have always been recognised but not been explicitly formalised until recently. The European Standard for Safety Critical Software [11] in the rail sector is potentially the first to recognise and formalise human competence requirements in the context of high-integrity software development for railway applications. The tables in Annex B of the standard have ten normative role specifications in the development of high-integrity software for safety applications, namely

B.1: Software Requirements Manager

B.2: Software Designer

http://dx.doi.org/10.5772/62080

B.3: Software Implementer

B.4: Software Tester

B.5: Software Verifier

B.6: Software Integrator

B.7: Software Validator

B.8: Software Assessor

B.9: Software Project Manager

B.10: Software Configuration Manager.

For each one of the above roles, a template based on the UML Class for the role is developed to describe the minimum essential competence requirements in terms of attributes (qualities) and operations (key activities and responsibilities) in the development and deployment of safety critical software. Whilst these appear simplistic and potentially inadequate, the significance of recognising and incorporating human characteristics in a traditional process only standard cannot be under-stated. In this respect, the competence requirements in the safety critical software standard are just a start and a foundation for more elaborations!

In principle, many of the normative software roles are generic and can be modified and applied to hardware, sub-system and system aspects. In a complex and safety critical project, it is beneficial if not necessary to adopt a systematic approach to characterising, assessing and managing competence in the key roles since as a minimum; these will be required for sub-system and system level software developers where a fair proportion of the change will originate from. To this end, a Competence Assessment and Management System is an essential aspect of a credible strategy within the context of a safety critical programme.

7.3. Competence Assessment and Management, a Systems Approach

Given the six facets of competence elaborated earlier under 7.1, the acquisition, assessment, development and management of competence poses a challenge beyond the traditional education and curriculum vitae. Whilst a blend of all six facets is a pre-requisite for competency and mastery in a given discipline, the significance of each is highly dependent on the context and requirements of a given domain. Whilst theoretical knowledge plays a more significant role in abstract scenarios, experience of application, adaptability and creativity may become more prominent in other domains. Whatever the domain, however, a systems framework for the evaluation, development and enhancement of competence is called for. This by necessity comprises two inter-dependent framework one focused on evaluation and assessment and the other on the management of competence.

7.3.1. Assessment of Competence

The competence assessment framework provides an integrated perspective on competence in a given context whilst additionally empowering the duty holders or the organisation to

benchmark each aspect, measure, assess and where necessary take actions to enhance various elements in the framework. [20] This is illustrated in the Weighted Factors Analysis (WeFA) schema of Figure 7. The latter aspects of benchmarking, evaluating, assessing and potentially enhancing competence are inherent in the underpinning WeFA methodology [12] and not elaborated here. The Schema details are omitted and elaborated in the subsequent section.

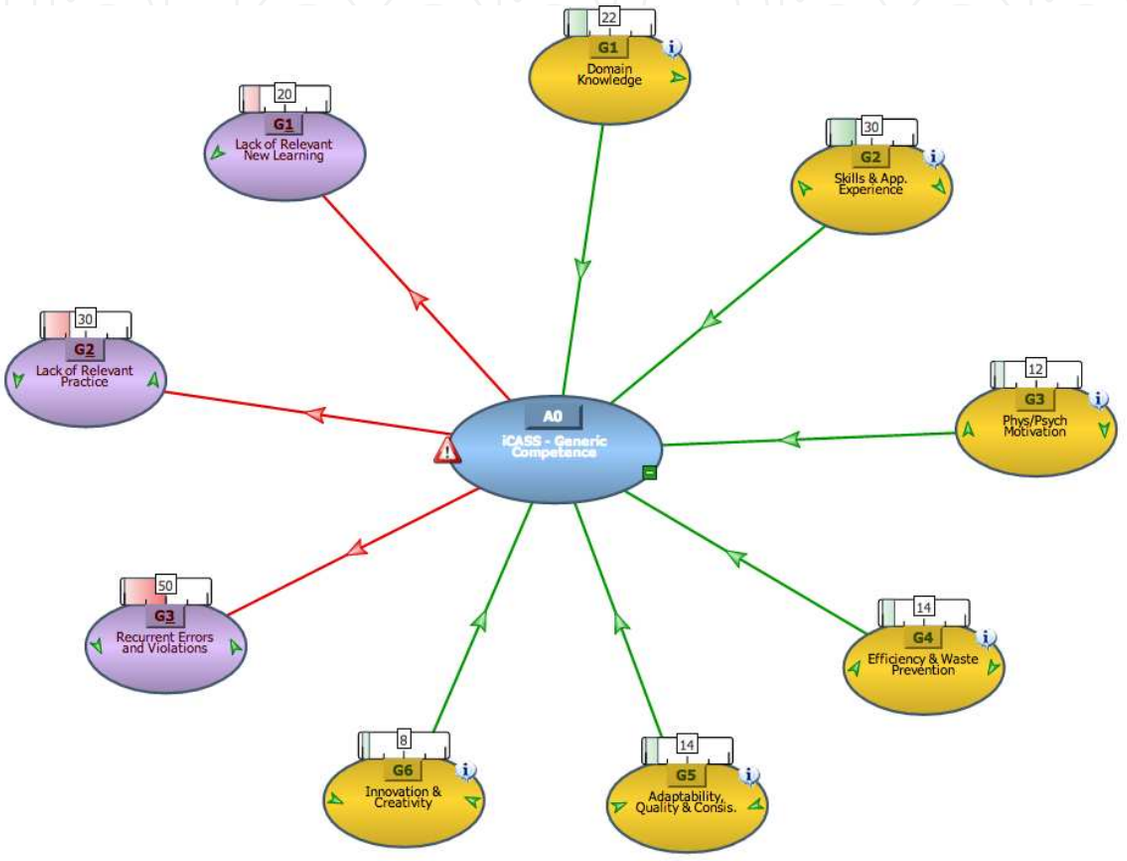

Figure 7. The Systemic Competence Assessment Framework

The determination, benchmarking, evaluation and quantified performance assessment of six drivers and three inhibitor Goals in the above WeFA schema is carried out as follows

7.3.1.1. Driver Goals

The requisite 'domain knowledge and understanding' in a given context as depicted in the driver Goal 1 (G1) is broadly supported by relevant industry's skill/competence frameworks. There are a number of such frameworks in use largely within various engineering disciplines in the United Kingdom, for example OSCEng, [13] IRSE [14] and IET [15]. Given the poor state of attention to competence and systematic approaches to its recognition, evaluation and assessment internationally, United Kingdom appears amongst the leading proponents globally [16].

http://dx.doi.org/10.5772/62080

The composition and extent of 'skill and relevant experience' in a given context as depicted in the driver Goal 2 (G2) in the assessment framework is supported by subsequent decomposition of G2 into lower-level WeFA structures, the so-called Level 2 and Level 3 goals. This principally helps determine the driver and inhibitor goals for the higher-level goal, the domain experience.

The requisite 'psycho-physical factors and behaviours' in a given context as depicted in the driver Goal 3 (G3) in the framework is supported by subsequent decomposition of G3 into lower-level WeFA structures in WeFA. This principally helps determine the driver and inhibitor goals for motivational, behavioural and drive aspects.

The essential determinants of 'efficiency and waste minimisation' in carrying out tasks in a given context as depicted in the driver Goal 4 (G4) in the framework is supported by subsequent decomposition of G4 into lower-level WeFA structures that drive or inhibit this goal.

The key determinants of 'quality, excellence and consistency' in carrying out tasks in a given context as depicted in the driver Goal 5 (G5) in the framework is supported by subsequent decomposition of G5 into lower-level WeFA structures, drivers and inhibitors, respectively.

Finally, the degree of 'adaptability, innovation and creativity' in a given context as depicted in the driver Goal 6 (G6) in the framework is supported by subsequent decomposition into lower-level factors relevant to this focus.

Given the hierarchical nature of WeFA schema, the so-called level 1 goals in the proposed individual competence assurance system are generic and universal. The decomposition of these goals into appropriate drivers and inhibitors in levels 2 and beyond will help tailor the generic model towards specific requirements of a given role in a given context. The driver and inhibitor goals in levels 2 and below in a competence role schema denote the specific measurable predictors for generic level 1 goals such as knowledge, experience.

Once a role is completely characterised through decomposition of the generic model (level 1) into a number of predictors (levels 2 and below), the schema is subsequently weighted by the same expert panel that have helped with the development of the schema. This assigns relative significance to the factors in the schema thus rendering it compatible with the values, preferences and possibly culturally driven norms within the application environment. A calibrated schema is then reviewed, enhanced and validated for general application within the context of use. In an automated environment, a validated/authorised schema can be assigned to every member of staff in a given role, enabling them to evaluate themselves against the criteria and develop a competence profile to establish the areas in need of further development.

7.3.1.2. Inhibitor Goals

The key aspects and the extent of 'lack or inadequacy of relevant new learning' in a given context of application as depicted in the inhibitor Goal 1 (G1) in the proposed framework is supported by subsequent decomposition into lower-level WeFA structures, the so-called Level 2 and Level 3 drivers and inhibitors.

The key predictors and the extent of the 'absence or inadequacy of relevant practice' in a given context as depicted in the inhibitor Goal 2 (G2) in the framework is supported by subsequent decomposition into lower-level WeFA structures.

Finally, the degree of 'recurrent errors and violations' in a given context as depicted in the inhibitor Goal 3 (G3) in the framework is supported by subsequent decomposition into specific predictors of these behaviours and outcomes in the schema.

A suitably developed and validated WeFA schema for competence assessment in a given role, context/domain additionally requires a measurement scale for each goal (driver or inhibitor) as well the weights, that is the strengths of influence(s) from each goal, on higher-level goals. Once established, the weighted framework lends itself to application for assessment and management of individual's or groups' competence in fulfilling tasks in the particular context as depicted by the framework. This would render a number of advanced features and benefits, namely

- Up to five levels of competence comprising apprentice, technician, practitioner, expert, leader in a given role/domain;
- Identification of the gaps and training/experience/mentoring requirements;
- A consistent and systematic regime for continual assessment and enhancement.

It should be noted that assessment here is devised and intended as a tool in the service of systematic approach to staff development and should not be misconstrued as an adversarial instrument for classification of people's contributions to the organisation.

7.3.2. Management of Competence

The deliverables of the engineering process applied to the creation and realization of parts, products, systems or processes often follow a life cycle from concept to decommissioning as popularised by engineering standards as detailed in Section 2.

In this spirit, the human resource involvement/employment within an engineering environment, organisation or project likewise follows a life-cycle comprising seven key phases essential to the systematic and focused management of knowledge, [20] namely

Proactivity comprises corporate policy, leadership, mission, objectives, planning, quality assurance and commitments to competency and service delivery for the whole organisation;

Architecting and profiling which comprises specification and development of a corporate structure aligned with the strategy and policy objectives together with the definition of roles and capabilities to fulfil these;

Placement which essentially involves advertising and attracting candidates matching the role profiles/requirements involving search, selection and induction. Selection relates to deriving role focused criteria and relevant tests to assist with the systematic assessment, scoring and appointment tasks. Induction involves a period of briefing, familiarisation and possibly training the extent of which is determined by the familiarity and competence of the individual concerned and the complexity and novelty of the role;

http://dx.doi.org/10.5772/62080

Deployment and empowerment which involves a holistic description depicting the scope of the responsibility, accountability and technical/managerial tasks associated with a specific role and empowering the individual to fulfil the demands of the role. This would include training, supervision, coaching, resourcing, delineation of requisite authority and accountabilities, mentoring and potential certification as means to empowerment for achievement and development;

Appraisal which involves the planning and setting performance objectives, and identification of the performance indicators/predictors synergistic to the demands of a role and the individual's domain knowledge, aimed at ensuring all relevant and periphery aspects of the role are adequately addressed and the necessary provisions are made for learning where a need is identified. The evaluation and appraisal provides the necessary feedback on compliance with individual and organisational objectives and achievement, enabling the organisation to identify and reward good performance and develop remedial solutions where necessary;

Organisation and culture which involves clarification of role relationships and communications, support, reward and motivational aspects for competency development including requisite resources and learning processes for attaining the policy objectives. This is intended to develop and foster a caring and sensitive approach/culture nurturing talents and paving the way towards an innovating organisation;

Continual development and progression: this comprises identifying the synergistic aspects which may serve as a complementary and rewarding extension to individuals'/teams' specific roles. Development may involve managerial, technical, support functions or an appropriate blend of duties at the whole life-cycle level or extensions to the role-specific activities and vision/ career paths above an existing role into other parts of an organisation and even beyond. The review and assessment of success in all the principles inherent in the framework also fall within the continual development principle.

The seven focal areas/principles constitute a systematic competency management framework. It is worth noting, however, that employment and project/product life cycles are orthogonal in that securing the requisite human resource and competence for any phase of an engineering production activity would potentially involve all the seven phases of the competence management.

The traditional process-based prescriptive rules and standards [4] have served the industry over a century where product and system complexities were generally low permitting good design and sufficient testing to ensure integrity of products, processes and systems. The pervasive complexities arising from adoption of new ICT technologies have necessitated a continuous approach to assurance throughout the life cycle as advocated by modern standards. This is now the accepted norm in the most safety and mission critical applications and industries.

Alas, the significance and role of the human agent has been largely ignored so far on the unfounded assumption that a recipe given to any capable and qualified person will ensure quality and integrity of the outcomes. With the ever increasing embedded knowledge contents in most products, processes and systems, the necessity to focus on the humans as the source

of such creation, and their fitness for the task in hand is now gaining momentum. In the face of such realisation and demands, our capacity to understand, characterise and evaluate human capabilities and latent potential has lagged significantly behind other technological advances.

We posit that human competence should be regarded as an integral facet of assuring designs, products and services, especially those with safety, security, sustainability or mission critical profile. The continual assurance processes advocated by modern standards need to complemented with focus on human competence to face the modern challenges of high risks and ever increasing complexity. The framework offered uses systems thinking to address assessment and management of competence within a coherent solution for enhancing quality, safety, reliability and assuring integrity.

8. General Trends and Emerging Issues

The statistics published by the Office of Rail Regulation (ORR) in the United Kingdom [17] is a timely reminder of the rise in passenger demand over the recent past that seems to illustrate a rising trend of roughly 50% per decade (Figure 8).

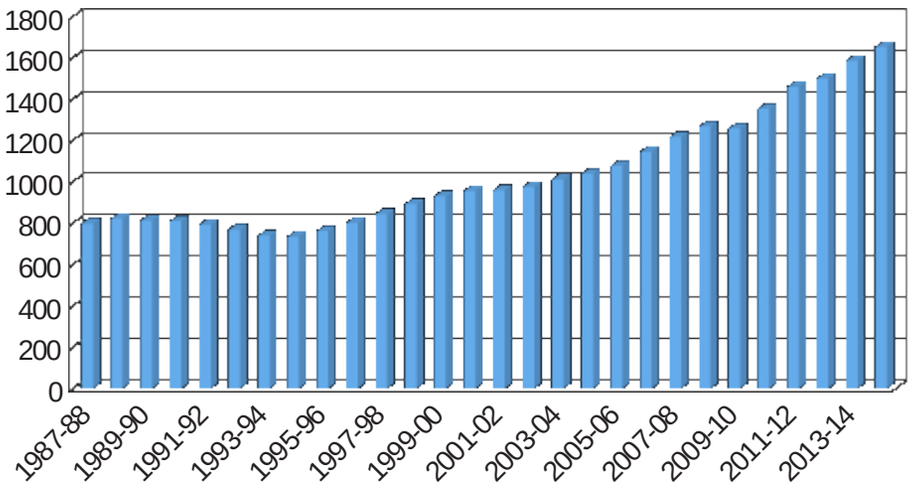

Figure 8. Rise in UK Railway Passenger Demand (ORR data)

Data from the World Bank relating to a rather similar period [18] seem to pint to a rising trend especially in the developing economies (Figure 9).

Overall, rise in global demand for rail transportation needs to be matched by increasing infrastructure investment, technology development and rising consciousness about the carbon foot print and global warming impact of transportation. Given the highly advantageous position of rail transportation with respect to sustainability, energy efficiency, carbon footprint, convenience and the increasing speeds, this is a growth industry on a competition course with the airlines.

http://dx.doi.org/10.5772/62080

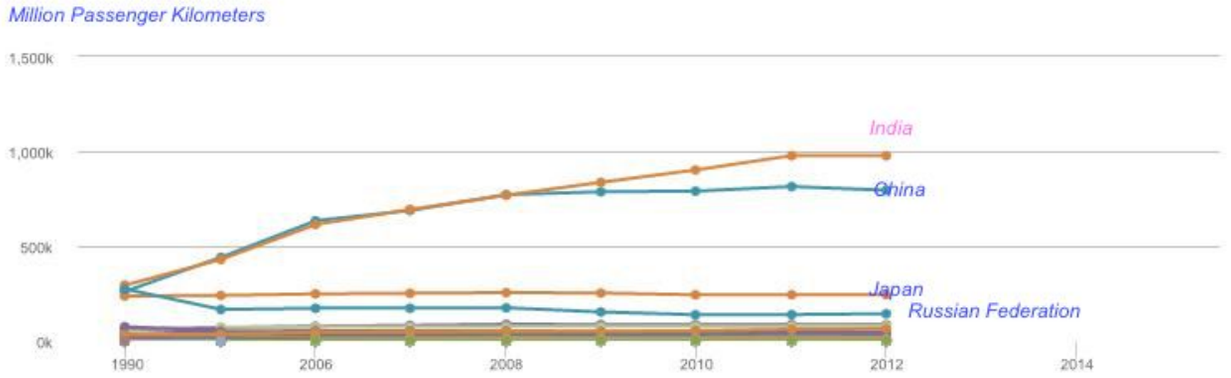

Figure 9. Rise in Global Railway Passenger Demand (World Bank Databank)

With the advancing technology, increasing automation, land speeds and demand for higher levels of safety, the key issues facing the industry from a safety and security perspective will be

i. Safety and security assurance of complex communications, supervisory and control systems comprising advanced hardware, hugely intricate heterogeneous software including some COTS components and vast amount of data.

ii. Integration of diverse multi-sourced inter-operable systems into a safe operational railway system.

iii. Understanding, addressing and monitoring of organisational and culture aspects of the human dimension.

iv. Developing and adopting advanced evidence driven scientific frameworks for evaluation, assessment and certification of railway products, services and systems.

v. Integration of safety and security assessment and management frameworks [19] for enhanced effectiveness, efficiency and cost reduction.

vi. Standardisation and harmonisation of operational rules across international borders.

vii. Developing common methods and metrics for the evaluation and assessment of safety and security.

Finally, with the maturity of the ICT technologies employed and improvement of safety performance, the concern will shift towards security as a more likely cause for incidents and accidents than the traditional concern over safety. Increasing levels of automation in train driving, traffic management and control would expose the future railway environment to a range of security threats that may take the operators, IMs and the authorities by surprise unless security, alongside safety is taken into account throughout the life cycle of products, systems and processes.

To this end, a similar reference portfolio as developed for the UK national railway's safety hazards is required to address security threats and vulnerabilities at railway system level. This

will provide a rational, systematic and consistent support to the operators and the supply chain in the industry empowering them to effectively address the security requirements pertinent to the scope of their services, products, systems and processes.

9. Abbreviations

CBRN Chemical, Biological, Radiological and Nuclear (attacks)

CDL Central Door Locking

CDM Construction, Design and Management (regulations)

Comms Communications

ConOps Concept of Operations

COTS Commercial-Off-the-Shelf

CRS Customer Requirements Specification

CSC Certificate of Safety Conformity

DRACAS Data Reporting and Corrective Action System

EMC Electro-Magnetic Compatibility

FMECA Failure Mode Effects and Criticality Analysis

FRACAS Failure Reporting and Corrective Actions System

FSaR Functional Safety Requirements

GDP Gross Domestic Product

HAZAN Hazard Analysis

Hazid Hazard Identification

HAZOP Hazard And Operability Study

HRC Human Resource Competence

HSE Health and Safety Executive (UK)

HW Hardware

IHA Interface Hazard Analysis

IP Intellectual Property

ISA Independent Safety Assessor

IT Information Technology

O&M Operation and Maintenance

OHA Operational Hazard Analysis

OHL Over-Head Line

Ops Operations

OPSEC Operational Scenarios

OSHA Operation and System Hazard Analysis

PHA Preliminary Hazard Analysis

PSP Product, System or Process

PW People-ware, the human element in a control system

QMS Quality Management System

RAM Reliability, Availability, Maintainability

SDS System Design Specification

SDSS System Design Safety Specification

SHA System Hazard Analysis

SSHA Sub-system Hazard Analysis

SIL Safety Integrity Level

SLSR Railway System Level Safety Requirements

SMS Safety Management System

SMIS An old UK Safety Management Information System data base

SRS System Requirements Specification

SSHA Subsystem Hazard Analysis

SSRS Subsystem Requirements Specification

SW Software

THR Tolerable Hazard Rate

UML Unified Modelling Language

V&V Verification & Validation

VTR Validation Test Report

Author details

Ali G. Hessami*

Address all correspondence to: a.g.hessami@ieee.org

Vega Systems, London, UK

References

[1] BS EN 50129:2003, Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling.

[2] BS ISO/IEC 15288:2002, Systems engineering. System lifecycle processes.

[3] CLC/TR 50451:2007, Railway applications. Systematic Allocation of Safety Integrity Requirements.

[4] Hessami, A. (1999). Safety Assurance, A Systems Paradigm, Hazard Prevention. Journal of System Safety Society, Volume 35, No. 3, pp. 8–13.

[5] Risk Profiling of Railways Report (1997). Can access a copy that includes the Hazards Portfolio at: https://vegaglobalsystems.com/Resources.html. Look in Public Resources/Safety Research online library for the file.

[6] European Guide to Good Practice in Knowledge Management, Work Item 5: Culture Working Draft 6.0, CEN-ISSS, July 2003.

[7] http://www.businessdictionary.com/definition/

[8] Managing health and safety in construction, Construction (Design and Management) Regulations (2007). (CDM) Approved Code of Practice, HSE Books, ISBN 9780717662234.

[9] Railway Safety Principles and Guidance: Part 3 Section A (2002). Developing and Maintaining Staff Competence HSG197, HSE Books, ISBN 0 7176 1732 7.

[10] +Safe Version 1.2, A Safety Extension to CMMi-DEV Version 1.2, Defence Materials Organisation, Australian Department of Defence, March 2007.

[11] BS EN 50128:2011, Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems.

[12] Hessami, A. and Gray, R. (2002) Creativity, the Final Frontier? The 3rd. European Conference on Knowledge Management ECKM 2002, Trinity College Dublin, 24–25 September 2002.

[13] OSCEng (2006). The Occupational Standards Council for Engineering publishes Occupational Standards for Engineering and Manufacturing (www.osceng.co.uk).

[14] IRSE (2007). Institution of Railway Signal Engineers Licensing Scheme (www.irselicences.co.uk).

[15] IET (2007). Competence Framework – Assessing Competence, The Institution of Engineering and Technology, UK (www.theiet.org/careers/cpd/competences).

[16] ORR (2007). The Office of Rail Regulator Railway Safety Publication No 1 Developing and Maintaining Staff Competence.

[17] ORR (2015). http://orr.gov.uk/statistics/published-stats/statistical-releases

[18] World Bank (2015). http://databank.worldbank.org/data/

[19] Hessami, A.G. (May 2004). A Systems Framework for Safety & Security – The Holistic Paradigm. Systems Engineering Journal USA Volume 7, No 2.

[20] Hessami, A.G. and Moore, M. (2010). Manage Competence Not Knowledge, Integrated Systems Design and Technology 2010, Knowledge Transfer in New Technologies, Springer, ISBN 978-3-642-17384-4.

IntechOpen