Complexity, Emergence and the Challenges of Assurance
The need for a Systems Paradigm

Prof A. G. Hessami[2] , Prof. N. Karcanias[1]

Systems & Control Centre, City University[1]
IEEE SMC Systems Safety & Security Technical Committee[2]

Abstract *–The complexity of modern products, systems and processes makes the task to identify, characterise and provide sufficient assurance about the desirable properties a major challenge. Stakeholders also, demand a degree of enhanced confidence about the absence of undesirable properties with a potential to cause harm or loss. The paper develops a framework of seven fundamental facets of performance as an ontology for emergent behavioural properties and a separate framework for the emergent structural properties of complex systems. The emergent behavioural aspects are explored and we develop a systems framework for assurance based on an Assessment and Management paradigm each comprising a number of principles and processes. The key argument advanced is that in the face of complexity and incessant change, enhanced confidence in the achievement of desirable and avoidance of undesirable properties requires a systems approach empowered by suitable modelling and relevant diagnostic tools explaining the nature of emergent properties. The principal focus of this paper is on safety, security and sustainability emergent behavioural (performance) aspects of complex products, systems and processes.*

Keywords: Safety, Security, Complexity Sustainability, Assurance, Systems Approach

I. Introduction

Amongst many challenges arising from the pervasive complexity in most modern products, systems and processes is the necessity to identify, characterise and provide sufficient assurance about the desirable properties. Alongside this, most key stakeholders, specifically the regulators and end users, demand a similar degree of enhanced confidence about the absence of undesirable properties often with a potential to cause harm or loss, for such products, systems or processes. We develop and propose a framework of seven fundamental facets of performance as an ontology for emergent behavioural properties and a separate framework for the emergent structural properties in complex and/or large scale system of systems. Understanding and managing complexity, as well as characterising structure are central to this work. The need for conceptualisation, analysis, assessment and enhanced confidence in the properties of complex systems, specifically the emergent behavioural aspects is subsequently explored where we develop and propose a systems framework for assurance based on an Assessment and Management paradigm each comprising a number of principles and processes. The key argument advanced is that in the face of complexity and incessant change, enhanced confidence in the achievement of desirable and avoidance of undesirable properties itself requires a systems approach, supported by appropriate modelling tools and diagnostics. These are needed to understand the nature of emergent properties as features of aggregation in complex processes and thus help us to avoid making erroneous decisions with costly and sometimes irreversible consequences. The principal focus of this paper is on safety, security and sustainability emergent behavioural (performance) aspects of complex products, systems and processes, but the framework has more general validity.

II. Complexity and Emergent Properties

Complex Systems is the term that emerges in many disciplines and domains and has many interpretations, implications and problems associated with it. The specific domain provides dominant features and characterise the nature of problems to be considered. A very significant class of complexity issues is that linked to design and operation of industrial systems. The distinguishing features of this area is the close link between modelling, system structure and properties, measurement-information and control-decision making-management structures which requires a systems framework.

Systems complexity is multidimensional and progressing beyond the stage of problem

conceptualization is a challenge. In this paper our interest is focused on aspects of systems performance. Much akin to most products and systems, the performance of complex systems is a measure of their utility, output and perceived or real emergent properties. The key facets to a general system's properties can be summarized as;

- Characterisation and Management of Complexity;
- Emergent structural properties;
- Emergent behavioural properties.

Problem complexity is manifested in many different ways which include:

(a) Lack of knowledge, or difficulties in characterising the behaviour of the basic process (*Unit Behavioural Complexity*).
(b) Complexity of computational engines (*Computational Complexity*).
(c) Difficulties in characterising the interconnection topology of sub-processes and/or variability, uncertainty of this topology during the system lifecycle (*Interconnection Topology Complexity*).
(d) Large scale dimensionality (*Large Scale Complexity*)
(e) Heterogeneous nature of sub-processes, resulting in hybrid forms of behaviour (*Hybrid Behavioural Complexity*).
(f) Organisational alternatives for the functioning, information and decision making (control) structures in respond to goals and operational requirements (*Organisational Complexity*).
(g) Variability and/or uncertainty on the system's environment during the lifecycle requiring flexibility in organisation (*Lifecycle Complexity*).

Emergent properties is a term referred to aggregate aspects of behaviour of the system properties. Frequently, such properties are linked to specific metrics defined by the system variables. The emergent behavioural properties of complex systems comprise an ontology of seven often context sensitive facets namely: **(1)** Technical functionality; **(2)** Cost; **(3)** Environmental behaviours & Sustainability; **(4)** Reliability, Availability, Maintainability; **(5)** Safety & Security; **(6)** Quality; **(7)** Perceived Value.

The above emergent behavioural properties or facets of performance are reasonably distinct and often inter-related thus posing a major challenge to designers, and duty holders to arrive at optimum solutions which satisfy stakeholders' expectations on each dimension. The evaluation of the degree of presence, or absence of these properties and the nature of interrelationships between them is an open problem that frequently depends on the nature of the specific system. One key distinction between these emergent properties is the fact that apart from safety and increasingly security and environmental performance, which are subject to a regulatory framework in most societies, the desirable level for the rest of these properties e.g. cost, reliability, quality etc. are left to the discretion of the duty holders and market forces. This therefore creates a legal compliance issue for attaining and assuring certain characteristics as well as deliver the corporate social responsibility.

The key differentiation between safety and security performance in cybernetic systems is broadly as follows; safety is freedom from harm to people caused by unintentional or random/systematic errors and failures of a product, process, system or mission whilst security is freedom from loss caused by deliberate acts perpetrated by people. Therefore security is principally characterised by intent and nature of causation as opposed to strictly being an output performance indicator reflecting degrees of loss or gain. Like safety performance, security of a system is mainly measured probabilistically in terms of risk due to inherent uncertainties. For simplicity, we deliberately exclude the so called natural causes or acts of god, in this analysis.

The security of general systems is often forecast and measured in terms of perceived or real threats and vulnerabilities and not in terms of consequential risk of harm and loss however. The threat is often an external source of malicious intent whereas vulnerability is an inherent flaw/dysfunction in a system making it prone to external and sometimes internal threats. Whatever the shortcomings on both aspects of safety and security performance, there's a discernible lack of systemic approach in identification, assessment and management of such risks in most enterprises and endeavors. This paper develops an systemic framework for assurance of safety, security and potentially sustainability in complex systems whilst proposing an innovative set of performance criteria for these critical facets of performance.

III. Systems Safety & Security, the Fundamentals

A. System Safety Concepts

The classical view of safety performance in hard and soft systems [5] is often biased towards historical accidents and often feeble post mortem attempts at understanding the causation and prevention or avoidance of similar causes. This deficient and primordial paradigm is challenged on the grounds that:

- Same accident may arise from a multiplicity of different causative factors;
- Accident investigations are predominately driven by legal imperatives and the need for finding a responsible person/body as opposed to the systemic understanding of the underlying root causes;
- Increasing pace of change, innovation and complexity in modern systems creates opportunities for new forms of accidents as yet un-encountered;
- The social, legal and organizational costs associated with accidents are constantly on the rise in view of the increasing public awareness, regulation and the litigation process.

It is argued therefore that allowing accidents to happen and the subsequent often inconclusive and feeble attempts at investigation and learning is tantamount to negligence and admission of failure in the face of challenges and risks faced. A new advanced paradigm based on credible and objective scientific principles is needed to counter the formidable risks posed by modern innovations, complex undertakings/missions and discoveries.

(1) The Systems Approach to Safety

In view of the major shortcomings of the dysfunctional classical accident focused approach cited above, the systems approach to specification, realisation and management of safe and secure systems is founded on the identification of hazardous states, generally precursors to accidents. This generates a deeper insight in complex systems and can expose a vast array of faults, errors, failures and vulnerabilities which individually or in combination lead to the realisation of hazardous states. Likewise, a hazard focused approach provides the opportunity to objectively scrutinise the potential escalation scenarios associated with a hazard and devise potent solutions to detect, contain, control or mitigate the broad range of accidents which may arise from such states in a general system.

In sharp contrast to the reactive learning from accidents, the systems approach to safety assurance principally focuses on empirical as well as creative identification of hazards. Once a suite of key hazardous states are proactively identified and ranked, it explores their causes, random or systematic [7], scrutinises their escalation scenarios and devises risk control and mitigation strategies [1]. Crucial for this approach is the need for a general systems framework that defines the relevant states.

(2) The Need for System Safety Metrics

Safety is a human focused concept reflecting the degree of freedom from unacceptable harm to people. Paradoxically, it is often measured by its absence for example, the safety of products, processes, systems and missions is regularly quoted in terms of risk of harm they may cause/entail to specific groups as opposed to the expected duration of harm free operation akin to reliability! The other fallacy is to forecast the safety of a complex system principally based on the empirical or past performance of similar systems, a notion which relates to random rather than systematic causes of hazards naively assuming that the future is a simple (linear) evolution of the past.

Safety is predominately measured in terms of risk which is a forecast comprising the likelihood/frequency of an accident and the degree of loss that it may entail. This poses a challenge to many duty holders or system designers who find it difficult if not impossible to relate the faults and failures of their products or systems to likely injuries and fatalities to the end users. To this end, some system standards [7] have advocated hazard rates as a direct measure of system safety, leading to the classification of system's safety properties in terms of Safety Integrity Level (SIL). The SIL concept which has a widespread following in the industry is more akin to a reliability perspective and is a non-systemic convention without much regard to the consequences of the so called dangerous failures [9].

Some sector standards, strangely derivatives of the IEC system standard [7], such as those for safety critical transport [8] advocate Tolerable Hazard Rates (THR), taking into account a total systemic perspective and the notion of tolerability of risk. There's a need for systemic metrics which go beyond failure and additionally take into account exposure of

various groups at risk as well as the potential escalation scenarios and tolerability criteria [17]. The THR concept which is principally reliant on historical performance of systems goes a fair way towards this ideal but fails to explicitly address all requisite factors in one cogent metric.

Whatever the approach, there's a need for a portfolio of systemic lead as well as lag indicators for safety, security and sustainability of complex cybernetic systems. We will address this issue further in this paper.

B. System Security Concepts

Unlike safety, security has many different interpretations and contextual implications for its stakeholders. From a systems perspective, security is lack of susceptibility to malicious intent which may comprise; **(i)** Vandalism; **(ii)** Sabotage; **(iii)** Theft and fraudulent gain; **(iv)** Terrorism; or a combination thereof. Whatever the context, security or lack of it is principally characterized by the intent on causing harm therefore, it is currently at least, a mostly human focused issue. However, in the cybernetics domain, this may eventually become a concern between autonomous intelligent systems without direct human intervention in spite of the three laws of robotics as laid down by Asimov [6].

(1) The Systems Approach to Security

There are two fundamental facets to security of a general system. The extrinsic dimension or driver is *threat*, characterized by the real or perceived existence of people or systems with intention to cause harm and loss. The intrinsic dimension or counterpart is *vulnerability*. In this spirit, whilst threats are diverse and unlikely to be fully forecast, anticipated or controlled, vulnerabilities are characteristics of a general system (cybernetic or otherwise), which arise from lack of awareness to potential for harm from threats in the larger environment of operation. Frequently, vulnerability may be characterized as a structural system property linked to interconnection topology, or some system functionality with a critical role, or linked to external to the system factors (external influences). Defining system vulnerability in concrete terms requires diagnostics and an appropriate methodology.

In a synergistic manner to systems safety assurance cited earlier, the main thrust of systems security assurance therefore rests upon systematic identification of key vulnerabilities, analysis of the causations and potential escalation scenarios and evaluation of pertinent risks. This is followed by proactive development of elimination or control strategies for major vulnerabilities and identification of detection, containment or mitigation solutions in the event of realisation of threats. However, in a similar manner to the systems safety related precursors (hazards), vulnerabilities as an intrinsic facet of a system's architecture or operation are mostly a concern at the system boundary. A further elaboration of this may lead to the consideration of internal and external threats and vulnerabilities with major implications for systems security which is beyond the scope of the current debate. In Systems of systems (SoS) or large open systems with significant degree of vulnerabilities, security is often assured through focus on threats rather than vulnerabilities. However, combined treatment of the intrinsic and extrinsic facets of the system are preferred where practicable.

(2)The Need for System Security Metrics

Bearing in mind the extrinsic and intrinsic facets, it is instructive to identify, quantify and treat threats and vulnerabilities collectively to ensure completeness and coverage of key concerns. Threat as an extrinsic measure for a system's security is generally classed into a number of distinct levels. The US Department of Homeland Security defines five Threat Conditions, each identified by a description and corresponding colour. From lowest to highest, the levels and colours are:

(a) Low = Green; **(b)** Guarded = Blue; **(c)** Elevated = Yellow; **(d)** High = Orange; **(e)** Severe = Red.

However, these are principally threat criteria relating to terrorism. The higher the Threat Condition or index, the greater the risk of a terrorist attack where risk includes both the probability of an attack occurring and its potential losses.

In a similar manner to the threats, metrics are called for systems vulnerabilities since these render a system susceptible to damage and harm, even in the absence of malicious intent at the outset. Even though the safety concept of SIL is not truly indicative of safety properties of a complex system [9], it is more appropriate for measurement of vulnerability since this is an intrinsic (architectural, compositional and operational) system

property. A credible metric for a cybernetic system's vulnerability would provide an objective measure of its resilience against potential threats. This could be a *System Resilience Index* which needs to be elaborated and quantified for various classes of vulnerability.

C. System Sustainability Concepts

(1) The Systems Approach to Sustainability

Sustainability is a high level emergent system property that expresses the ability of the system to survive and continue to function according to the original goals set for its operation. It is thus related to :
(i) Robustness of the system behaviour to external disturbances ;
(ii) Ability to overcome threats that may have catastrophic consequences by demonstrating capabilities to survive and achieve the central goal ;
(iii) Adaptability by demonstrating capability to reorgonise its control and information structures after some catastrophic events, or changes in the operational goals of the system due to changes in the market ;
(iv) Potential for the system to evolve in a continuously changing environment of goals, specifications and constraints.

In principle, apart from survivability and résilience attributes, sustainability possesses social, economic and enviornmental dimensions as well, making it a complex composite property in its own right. It is clear therefore that the basic concepts required to define sustainability are themselves emergent system properties and it is this that makes sustainability a higher level emergent property.

(2) The Need for System Sustainability Metrics

Defining *sustainability* as an emergent higher level, or composite property implies that we need to: **(i)** Identify the constituent (primitive) emergent properties. **(ii)** Develop diagnostics for characterising and evaluating the primitive emergent properties. **(iii)** Develop a coneptual system framework expressing sustainability as composition, aggregation of simple-primitive emergent properties. **(iv)** Develop a meta-model expressing this aggregation and enabling the evaluation-measurement of sustainability.

Developing metrics for sustainability is a challenging problem that has to address all issues described above. The difficulties are due to the characterisation of primitive emergent properties in terms that may be quantified, as well as expressing the composition in a way that supports the development of composite metrics. These tasks are beyond the scope of this paper.

IV. Systems Safety, Security and Sustainability Assurance : the Framework

We propose two complementary and advanced sets of systems principles and processes as the underpinning backbone to tackling the challenges of safety, security and potentially sustainability in products, processes, systems and undertakings. Taking a life-cycle perspective [12] these comprise I & III below;

(i) Assessment: This comprises recognising the need, defining the system, specifying and identifying/understanding of key properties, behaviours, hazards and vulnerabilities, evaluating and assessing expected impact;

(ii) Realisation: This is ultimately aimed realising the desirable properties and achieving the desired performance in the form of product, process, system, mission or undertaking;

(iii) Management: this comprises taking the outcome of assessment and realisation into consideration and ensuring deployment, delivery of requisite performance, continued monitoring and control through a responsive and holistic suite of strategies, resources and actions.

Whilst Realisation is specific to a given domain and context, the Assessment and Management aspects as a suite of principles constitute a meta-knowledge framework which can be abstracted and developed for almost universal application across many domains and disciplines. The systemic framework of assessment and management is equally applicable and effective within the context of desirable as well as undesirable properties of products, systems and endeavours. This is contrary to the current conventional wisdom where specification, delivery and continual monitoring of desirable aspects of performance is regarded as an essentially domain expertise where as the undesirable and unintended emergent properties (hazards and vulnerabilities) are the forte of so called risk management. The +Safe3 extension [11] to the renowned CMMi model [14] also distinguishes between Safety Engineering & Safety Management, which are mainly synonymous

with Risk Assessment and Risk Management advocated here.

Whilst presented as a dual and complementary suite of principles and processes, assessment and management are iterative and systemic in the sense that processes inherent in the management framework employ assessment activities at requisite points to support judicious decision making and ensuring optimal performance. These are collectively referred to as *Systems Assurance* and labeled as *Surety Framework* in this paper.

A. Risk Assessment

This key facet of Surety framework depicted in Fig. 1 is proposed as a backbone to the identification, specification, evaluation and assessment of the undesirable events or properties adversely affecting technical functionality, cost, reliability, safety, quality etc. The risk assessment process [13] comprises seven systemic aspects such as: **(a)** Hazard Identification; **(b)** Causal Analysis; **(c)** Consequence Analysis; **(d)** Loss Analysis; **(e)** Options Analysis; **(f)** Impact Analysis; **(g)** Demonstration of Compliance.

The risk assessment process, whilst systematic and comprehensive, is aimed at enhancing the systemic understanding of the key issues and is not treated as an end in itself. Assessment process generates transparency and awareness of real and potential issues thus empowering the duty holders to take appropriate actions and make the transition from fire fighting and reactivity to anticipation and proactivity.

B. Risk Management

A holistic and systemic approach to assurance of safety and security properties of generic products, processes, systems or undertakings is developed and proposed in a major paper [4]. The paper elaborates seven principles which have to be collectively fulfilled before sufficient assurance is gained and maintained in the desirable safety and security properties of a general or cybernetic system.

This complementary aspect of assurance within the Surety Framework comprises an advanced and systematic approach to developing, sustaining, enhancing and managing the so called downside events and properties associated with any complex product, process, system or undertaking. Risk management builds upon the outcome of systematic assessment and ensures the identified and prioritized risks are eliminated, mitigated or continually controlled in a comprehensive and responsive manner. The risk management process is depicted in Fig. 2.

The proposed systems suite of principles demands a thorough and structured scrutiny of the problem domain as the key stage in safety/security assurance followed by a number of complementary and value added activities. The principles underpinning the systemic and holistic management of safety and security are;

(1) Proactivity; **(2)** Prevention; **(3)** Protection & Containment; **(4)** Preparedness & Response; **(5)** Recovery & Restoration; **(6)** Organization & Learning; **(7)** Continual Enhancement.

The nature and essential aspects of the principles are detailed in the published paper [4]. However, the suite of seven principles is equally applicable to cybernetic systems in which, in view of the complexity (spatial or temporal or both) or novelty, assurance is mainly derived from the quality of the process and competencies of those involved.

C. Application of the Framework

The systemic framework of assessment and management proposed here is applicable to the attainment, maintenance and continual enhancement of three key and increasingly regulated aspects of safety, security and the environmental performance/sustainability of general and cybernetic systems.

Nano-technology poses a modern and innovative domain where the safety and indeed security and the environmental implications of its products and offerings are largely unknown even by purveyors of the relevant products and services. An illustrative case involves the marketing of cosmetics containing nano-particles [10]. Because of their far smaller size, these particles are absorbed deeper into epidermis, dermis, cells and eventually into the blood stream of the users. The significant uncertainty on the risks has led to calls from the UK Royal Society and the US Federal Drug Administration (FDA) for a comprehensive research programme into the likely effects. In the mean time, the cosmetics industry considers nano-particles a “hot technology” with lots of intriguing applications, allocating vast sums to research into nano-technology. The FDA maintains that urgent research is called for due to the paucity of the knowledge on the effects

of the nano-particles when they enter cells in the human body or leach into the blood stream. A systemic framework constitutes a potent weapon in the face of such huge uncertainties with major implications for the human society at large.

The seven underpinning principles for risk management can be mapped to the requirements of any domain at any level of abstraction or details namely: **(i)** Industry / Sector; **(ii)** Corporate / Organization; **(iii)** Division / Team; **(iv)** Project / Product; **(v)** Mission. The scalable architecture for application of the proposed surety framework at macro (society/corporate) and micro (system/product) levels would entail:

(a) Identification of key influencing factors for each one of the seven principles and generation of a hierarchical network/model for such factors depicting their roles and relationships [2];

(b) Assessment and quantification of these networks and generation of an overall numerical index for each principle in the framework [3];

(c) Generation of a combined figure of merit (System Integrity and Resilience Index-SIRI) for the whole generic or cybernetic system under consideration, based on the seven indices derived for each principle.

Such indices can be benchmarked against desirable or tolerable levels of safety, security and environmental performance thus providing a reference level for the optimal assurance under each individual principle as well as the whole framework applied to a system. This generates an advanced, focused and responsive system for attainment, management and continual enhancement of safety and security properties at the pertinent application level.

V. Conclusions

Amongst the seven key facets of a system's performance cited earlier, the safety, security and the environmental/global aspects are increasingly regulated by governments [17,19]. This is partly driven by the gradual enhancement in the quality of life and public's awareness and demand for a more socially responsible stance by duty holders; private and public corporations, service providers and the suppliers. One of the striking observations in the fields of safety, security and environmental assurance is the overt reliance on often parochial technical solutions at the expense of a systemic and holistic understanding of the key issues and domain requirements.

Cybernetic systems driven by complexity, novelty and increasing pace of change and progression pose a challenge in safety and security if not environmental assurance due to inherent uncertainties. In such settings, the adoption of a systemic framework of universal principles assists with enhanced confidence in emergent properties where otherwise significant uncertainties prevail.

The proper development of the field requires a suitable abstract systems framework that can explain and provide model based tools and diagnostics for emergent system properties. This is crucial for the development of metrics that can characterize primitive and composite emergent properties. Metrics may provide characterization of such properties. Linking emergent properties to system structure is critical, if we are to address issues of re-engineering of systems and processes aiming for development of systems with improved desirable properties, or reduced risks. Reengineering for improved systems assurance is an area where future research has to develop. Such efforts, however, require an appropriate systems framework [15], [16] that can support analysis and design by following paths similar to those deployed for hard systems.

We have developed and proposed an integrated framework comprising assessment and management paradigms labeled as Surety. However, whilst the current focus has been the avoidance or minimization of risks, Surety framework additionally encompasses performance optimization not addressed here. Such systemic assurance frameworks are instrumental in holistic identification, classification and treatment of critical issues (hazards and vulnerabilities) and the specification/adoption of pertinent solutions. Founded in systems theory and embodying a significant structural, empirical and scientific knowledge, they also assist with the evaluation of the effectiveness of the risk control options whilst exposing gaps in the overall landscape and strategy. In view of the synergies between safety and security facets of performance, adoption of one integrated framework would result in savings on time and effort whilst optimising investment in equipment and systems. They are the most potent weapon in the face of epistemic uncertainty.

VI. Nomenclature

Assurance:
Increasing confidence and certainty

Gain: Lives saved, improvements made, damages prevented or avoided in the natural habitat or benefits accrued to a business/society or a combination thereof. The expected value of a future benefit.

Hazard: Object, state or condition which in the absence of adequate detection or containment could lead to an accident.

Health: Soundness of body and mind, freedom from illness

Loss: Physical harm to people, detriment to a business/society or damage/destruction of the natural habitat or a combination thereof.

Reward: A forecast for a desirable event or gain.

Risk: A forecast for an accident or loss. The expected value of a future loss.

System: A (purposeful) composite of inter-related parts / elements with discernible collective output(s) or emergent property(ies) not manifested by any of the elements.

Safety: Freedom of people from (physical) harm.

Security:
Freedom from vulnerability or loss caused by deliberate and malicious acts.

Sustainability:
A blend of social, economic and environmental considerations which render a product, system or undertaking viable and continually optimal.

Systems Assurance:
The art, science and technology of ensuring and demonstrating that a system is likely to achieve its objectives without engendering unacceptable levels of loss.

Systems Safety:
The art, science and technology of ensuring and demonstrating that a system is not likely to lead to unacceptable levels of (physical) harm to people.

Systems Security:
The art, science and technology of ensuring and demonstrating that a system is not likely to be vulnerable to malicious deliberate acts aimed at engendering unacceptable levels of loss.

Vulnerability:
Susceptibility to injury, fatality or loss.

Welfare: Well being and quality of life for individuals and the society.

VII. References

[1] A.G. Hessami, *Safety Assurance, A Systems Paradigm*, Hazard Prevention-Journal of System Safety Society, Volume 35 No. 3, third quarter 1999, pp8:13.

[2] A.G. Hessami, *Risk, A Missed Opportunity*, Risk and Continuity Journal, 1999, pp2:17-26.

[3] A. Hunter, and A.G. Hessami, *Formalization of Weighted Factors Analysis*, Knowledge-Based Systems, 2002.

[4] A.G. Hessami, *A Systems Framework for Safety & Security, The Holistic Paradigm*, Systems Engineering-The Journal of the International Council on Systems Engineering, Volume 7 Number 2, 2004, pp99-112.

[5] A. Waring, *Practical Systems Thinking*, International Thomson Business Press. 1996-ISBN 0-412-71750-6.

[6] R. Clarke, *Asimov's Laws of Robotics, Implications for Information Technology*, IEEE Computer 26- December 1993 pp.53-61 and 27, pp.57-66, 1- January 1994.

[7] IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems* - International Electrotechnical Commission, 20-Jan-2005.

[8] CENELEC, *European Standard EN50129 Railway Applications – Communications, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling*, February 2003.

[9] A.G. Hessami, *Risk Management a Systems Paradigm*, Systems Engineering-The Journal of the International Council on Systems Engineering, Volume 2 Number 3, 1999, pp156-167.

[10] Safety Fears over 'nano' anti-ageing Cosmetics, The Sunday Times, 17 July 2005.

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

[12] ISO/IEC15288, *System Life Cycle Processes* - ISO/IEC October 2002.

[13] Engineering Safety Management Issue 3 (Yellow Book III), Volumes 1 & 2, *Fundamentals and Guidance*, Railtrack PLC UK, January 2000, ISBN 0 9537595 0 4.

[14] M.B. Chrissis, M. Konrad, M, S. Shrun, *CMMI Second Edition, Guideline for Process Integration and Product Improvement*, ISBN 0321279670, January 2007.

[15]N.Karcanias, 2003. "*System concepts for General Processes: Specification of a new Framework*". Systems Research Centre Report, SRCRep-06-03/1, City University.

[16] N. Karcanias, 2008. "*Structure evolving systems and control in integrated design*" IFAC Annual Reviews in Control, Volume 32, Issue 2, December 2008, Pages 161-182, doi:10.1016/j.arcontrol.2008.07.004

Further Suggested reading:

[17] IEC 62278, *Railway Applications-Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS),* 9/686/FDIS, 2002

[18] *Successful Health and Safety Management – HSG65*, HSE Books, second reprint 2000, ISBN 0-7176-1276-7.

[19] Council Directive 96/48/EC: *Interoperability of the Trans-European High Speed Rail System*, 23 July 1996.

TSIs under Directive 96/48/EC

-2002/730/EC-Maintenance

-2002/731/EC-Control Command and Signalling Systems

-2002/732/EC-Infrastructure

-2002/733/EC-Energy

-2002/734/EC-Operations

-2002/735/EC-Rolling Stock

[20] Railway Safety Management System Guide, Railway Safety-Transport Canada, Ottawa-Ontario, February 2001.

[21] CENELEC, *European Standard EN50126 Railway Applications – The Specification and Demonstration of Dependability – Reliability, Availability, Maintainability and Safety (RAMS).*

[22] E. Okstad and P. Hokstad, *Risk Assessment and Use of Risk Acceptance Criteria for the Regulation of Dangerous Substances*, ESREL 2001

[23] Railways (Safety Case) Regulations 2000 including 2003 amendments, Guidance on Regulations L52, HSE Books.