Macrothink Institute™

Journal of Safety Studies
ISSN 2377-3219
2016, Vol. 2, No. 2

Safety; a system state or property?

John Stoop
Kindunos Safety Consultancy Ltd
Spijksedijk 8, 4207 GN Gorinchem, the Netherlands
Tel: +31 183 637484
Email: stoop@kindunos.nl

doi:10.5296/jss.v2i2.10446 URL: http://dx.doi.org/10.5296/jss.v2i2.10446

Abstract

Safety is frequently addressed as an emergent property of complex and dynamic systems. This contribution advocates the validity and importance of incorporating intrinsic technological hazards and systemic interrelations from a multi-actor perspective in the early phases of design and development. This perspective creates inherent properties in various system states, which may manifest themselves as emergent properties during operations. These safety properties are based on their business models, selectively focusing on primary system components such as infrastructure, vehicles or traffic management. Experiences with major aviation and railway projects highlight the potential of engineering design approaches such as multidisciplinary design optimization, value engineering and vectorial state/space modelling. Such an approach has high change potential for a specific category of high energy density complex socio-technical systems.

Keywords: safety, systems engineering design, emergent properties, railways, aviation

1. Introduction

In analysing complex and dynamic systems, safety is frequently considered an emergent property, to be disclosed in its actual performance during operational practice. In this contribution, we argue that safety is primarily an inherent property, defined and designed into systems from the conceptual phase on. Historically, safety in complex transport systems are defined by their accident and incident frequency and the unacceptability of major disruptions and catastrophes in the functioning of these public transport systems. Due to the decrease of accident frequency, the physical damage and injuries to users are challenged as an appropriate measure for their safety performance. Instead of looking what went wrong, we should shift to analysing what went right and adapt to a proactive perspective. This proposition of abandoning retrospective approaches in favour of prospective approaches is challenged from an engineering design perspective. Safety performance in complex systems is both determined by their societal goals and values, design principles, intrinsic and inherent properties and emergent operational performance from both a feedback and feed forward perspective. This contribution elaborates on the architecture and configuration of complex and dynamic systems, elaborating on their technological intrinsic hazards, multi-actor characteristics, business models, hierarchical control mechanisms, institutional arrangements, adaptive potential and network configuration dynamics. Several case studies in aviation and railways demonstrate that safety performance indicators can be traced back to each of such systems characteristics. They enervate the assumption of a linear, direct relation between safety performance, traffic volume and growth.

To this purpose, the contribution elaborates on the variety of modelling techniques and network typologies which are available for providing structure to understanding the dynamics in complex systems and the multiplicity of system states that are potentially available. Analysing the nature, tractability, stability and resilience of these states determines whether a system remains controllable and manageable across the variety of operating envelopes and transitions across these envelopes. The contribution demonstrates the validity of the notions of inherent properties and system states by case studies from the aviation and high speed line railway industry. The next three sections elaborate on the High-Speed Line (HSL) project as a multi-actor optimization with emergent safety issues, the SESAR project as a business model adaptation study into inherent properties and the stall recovery case study as a conceptual change case study dealing with safety as an intrinsic value.

2. The HSL project

In 1996 the Netherlands and Belgian government took the initiative to realize a high-speed railway connection between Amsterdam and Brussels. The project started in 1996 and was completed in 2012. In the Netherlands, the length of this line was 125 km, of which 85 kilometres were new and 40 km were existing railways. The line had to cross several large waterways with tunnels or bridges, and a large tunnel (nearly 8 km) had to be built to comply with environmental requirements. The Dutch and Belgian governments were commissioners for the project. The Dutch government made design and construct (DC) agreements with six

civil contractors, while a design, build, finance, and maintain (DBFM) agreement was made with an infraprovider, Infraspeed. The concession in the Netherlands was granted to High Speed Alliance, a daughter of the Dutch Railway Company.

The infraprovider had a design and construct department and a maintenance department that operated more or less independently. The Dutch High Speed Alliance and the Belgian NMBS needed dedicated high speed trains for the exploitation of the line. They ordered a set of trains with AnsaldoBreda in Italy. Part of this European Union initiative to open up markets was the development of ERTMS, the European system for train signalling. The technological requirements for rolling stock and infrastructure were harmonised in Technical Specification for Interoperability (TSIs). The first versions of these TSIs were published in 2002 (Walta, 2013). During the negotiations for the agreements with Infraspeed and HSA in 2000-2001 the TSIs were only available in draft without specifying the version. Between 2002 and 2009 the specification of ERTMS changed (Stoop et al., 2007). Due to the many coupled processes and actors, unexpected and unmanageable effects emerged, leading to an investigation (Stoop et.al. 2007). The exploration company ordered new trains that were designed specifically for this line for a maximum velocity of 250 km/h. The delivery of the new trains was severely delayed and the train service between Amsterdam and Brussels started in 2009 with modified Traxx locomotives and conventional carriages that could operate at 160 km/h.

The design and construction process of the trains were checked for compliance by a Notified Body. The design process however, was also closely monitored by a supervising team, in which the exploitation company was represented. This made the design of the train no longer a sole responsibility of the train manufacturer (Walta, 2013). The new trains did pass all European certification procedures but did however, encounter a lot of problems during the testing phase which continued in the first months of service in the end of 2012. This culminated during a few days of snow in the start of 2013, where trains lost a metal plate and caught fire in a battery pack. Altogether, the trains were operational for 40 days, leading to a parliamentary investigation (Toorenburg, 2014). The Belgian authorities withdraw the operational license for the Belgian part of the line, followed by the Dutch authorities. As a result, the NMBS cancelled the contract with AnsaldoBreda. All trains were returned to Italy in 2014. Up till now no high-speed trains operate between Amsterdam and Brussels. The high-speed line is now being operated with 160 km/h.

In its survey in 2014, the Algemene Rekenkamer (2014) counted 16 different parties involved in the project. The agreements that the government made with these parties after public tenders, all imposed a specific business model on the contract partners. The agreements with the civil contractors stressed the building costs and the realization time, because the work was granted to the contractors that offered the work for the lowest price with fees for late delivery. The agreement with the infraprovider stressed the availability of the line. The infraprovider had to finance the construction and was compensated for the availability of the line. The concession agreement with the exploitation company was granted to the highest bidder, which had to earn back their bid from the exploitation. Every actor optimized its part of the project within the limitations and the business model given by the specific contract. The

technological, legal and temporal interactions were neither well understood at the start of the project, nor corrected during the project.

The agreement between the central government and the infraprovider contained clauses that could cause financial claims if the government imposed measures on the infraprovider that influenced the performance of the line. These clauses made it difficult to coordinate technological solutions between the infraprovider, civil constructors and the exploitation company. Commissioning too many autonomous parties made project control difficult. Actors seemed to have higher interest in their own contractual obligations than in the success of the overall project. The assumption that it would be in the interest of the private parties to apply self-coordinate among their activities proved false. The private parties had an interest in trying to transpose the risks back to the government. It proved more profitable for parties to build a strong liability case for a lack of coordination than to adapt their own design in order to get a better overall solution.

The analysis shows that during the project coupling between processes –both temporal, technological and legal- gave rise to unexpected proliferation of perturbations (Algemene Rekenkamer, 2007; Van Kleef and Stoop, 2016). The commissioner had no oversight over these couplings and the overall system performance. The system proved to be safe, but neither available, nor reliable. A systems architect and dedicated problem owner with top-down oversight over the integral systems performance is indispensable with respect to infrastructure, signalling and rolling stock with powers to prioritize financial resources and allocate responsibilities.

3. Single European Sky

In order to accommodate sustainable growth, the European project SESAR is initiated by the European Commission. Such accommodation requires conceptual change towards a flexible use of airspace at an international level, controlled by the international organisation Eurocontrol (Eurocontrol, 2010). At present, airspace capacity management is a national responsibility, involving both Ministries of Transport and Defence, balancing a quantitative efficiency for civil use versus qualitative effectiveness for military use. At a high strategic level a Single European Sky should be realized by a transition towards a functional use of airspace. As an intermediate step towards a single European sky, the SESAR project is aiming at Functional Airspace Blocks, with methodological support for regulatory involvement in major changes and a satisfactory management of emerging safety and safety regulation risks.

The regulatory acceptance of change requires development of new scanning tools, primarily by the application of Safety Cases, with oversight responsibilities for ICAO and the EU. The national States in the EU act as regulators, providing instructions for compliance with competences and by prescribing structure by requiring functionalities and demanding confirmation by proof. Minor changes are to be checked within the system, while major changes require change in legislation. Liability is organised by contract while legal breaches are covered by taking precautions. Judging a breach is preventively addressed by jurisdiction,

applying the Care Principle on a case by case level across the life cycle of the system, addressing duties to responsible persons, objective attribution through compensation by licensing and implementation of a SMS, allocating responsibilities to actors, system parts and functions while a survey of causes of damage to the systems is providing oversight on hazards and risks.

Safety screening is conducted based on three criteria: Duty of Care, provided by Standards, Responsibilities addressed to actors, and creating Independent Oversight by a Public Authority (Eurocontrol, 2010). At a national level a prominent role is allocated to airline operators in planning capacity and balancing costs of air fares versus fuel savings (Offermans 2016). In the present European system crossing of active military zones is prohibited, due to which diversion of routes are required to avoid traffic conflicts. Future changes in the ATC system will see a transition from causal and empirical approaches to mathematical modelling of capacity demands. Air services are regulated through the State model of ICAO, although a considerable fluctuation is present in the tariffs and fares between States. Eurocontrol serves as a cashing agency, passing along the costs for transition through national air spaces. Assessing the safety performance of the SESAR project is only foreseen in the second phase of the project (2015-2019) by PRA and matured SMS approaches. In the first phase (2012-2014) no safety targets were available, while for the third phase (2019-2024) safety performance indicators are not yet available (Offermans, 2016).

The goal of a unified European air space is reduction of financial losses, based on automation and software driven algorithms, based on a financial business model. A Single European Sky reduces redundancy in air traffic control by reducing multiple centres to a single centralised air traffic control centre. Economic growth is accommodated by increasing the traffic flow density, design of and exploration of data to monitor margins and controlling the actual traffic flow. The SESAR concept aims at controlling traffic flows instead of supporting individual flight, reducing intervention to handling non-standard flight situations and synergies of chain effects. The business model is based on the position of the flight in the value chain as a cost factor, since fuel optimization options of the aircraft are almost expired. A shift to Air Navigation Service Providers occurs dealing with enroute costs, services provided and applying meridian flight routes. A reduction of workload is anticipated, focusing on traffic volume management, oversight, value engineering by creating homogeneous traffic flows, impacting flight kinematics, time punctuality demands and improved control over the system state and system variables. Safety consequences are to be assessed by influencing the kinematic flight process, managing uncertainties while maintaining oversight and handling of conflicts and undesired consequences.

At present, in reality however, the shortest routes available in Europe differ from the actual planning by a difference of 80000 nautical miles per day. Only 8% of all potential improvements are applied by airline operators for obvious reasons of reliability, cheaper route diversion options, limitations in crossing military zones and the use of standard flight plans (Apon 2016). The intermediate strategy to introduce Functional Airspace Blocks flawed due to national policies with respect to their tariffs in the earning model, maintaining military and

civilian corridors creating congestion and delays, optimization of individual airline operators in balancing fuel savings versus flight fare costs. Based on their economic interest, several countries in the EU are reluctant to accept the introduction of Functional Airspace Blocks. ATC in Europe covers 8.6 billion Euros, 57000 jobs of which 16900 ATC staff. Five countries cover about 54% of all air traffic with a peak during the summer period. The earnings of cross traffic tariffs are part of the State income. On the busiest routes, military restricted areas force deviations from the meridian optimum, creating dense traffic in restricted air space. National interests block a Single European Sky to a safer and greener air space with increased capacity. Privatisation, such as in the USA with the Next Gen ADS-b system, is a serious option that can create a merging towards solutions that are politically unfeasible (Offermans 2016).

In this transition to the SESAR and open architecture integrated cockpit avionics concept, crucial changes are introduced with respect to the actual operating practices of flight capacity planning and flow management based on software and design driven automation, design assumptions based on predefined business models and engineering based automation (Offermans, 2016). In such a software engineering based design concept, there is no room for operational experience and feedback of tacit knowledge of ATC staff.

In addition to conceptual changes in ATC, the introduction of open architecture integrated avionics in the cockpits, similar to the already existing military on-board equipment, will be able to create complete new mission profiles. Such Avionics Management Systems (AMS) enable singular and shared pilot displays with Heads-Up facilities that enable manipulation of weather radar, terrain mapping, airport charting engine and component health monitoring and additional flight environment and aircraft information. Such AMS will have multiple hardware and software abstraction layers that allow any part of the architecture to be modified or replaced with minimal system impact and recertification costs. New functions can be implemented and integrated based on each user's needs by management of the cockpit configuration and customizing AMS aspects. The concept discriminates static and volatile elements for the benefit of reducing the burden of re-certification (Avionics Magazine 2016).

Such a combination of innovating business model and open system architecture heavily relies on a failsafe equipment and flawless systems architecture with respect to the human-machine interface, conflict resolution and contingency handling. There are no tools nor precedents for testing and certification of such complicated, open architecture systems, while emergent properties in the form of catastrophic events are unacceptable. According to Minsky however, a drift into failure in a system transition period under conditions of risk-taking and innovation is likely to occur (Minsky 1986). The only alternative to such a drift is to analyse the intrinsic design principles and inherent properties during their design and development. In contrast with the Next Gen ADS-B developments in the USA, the SESAR project does not yet deal with Unmanned Aerial Systems as a new ATC challenge.

4. Stall, an intrinsic system property

From the early days of aviation, stall has been an inherent hazard. Otto Lilienthal crashed and perished in 1896 as a result of stall. Wilbur Wright encountered stall for the first time in 1901, flying his second glider. These experiences convinced the Wright brothers to design their aircraft in a 'canard' configuration, facilitating an easy and gentle recovery from stall. Over the following decades, stall has remained as a fundamental hazard in flying fixed wing aircraft.

Stall is a condition in which the flow over the main wing separates at high angles of attack, hindering the aircraft to gain lift from the wings. Stalls depend only on angle of attack, not airspeed. Because a correlation with airspeed exists, however, a "stall speed" is usually used in practice. It is the speed below which the airplane cannot create enough lift to sustain its weight in horizontal flight. The angle of attack cannot be increased to get more lift at this point and slowing below the stall speed will result in a descent. Airspeed is often used as an indirect indicator of approaching stall conditions. The stall speed will vary depending on the airplane's weight, altitude, and configuration. Fixed-wing aircraft can be equipped with devices to prevent or postpone a stall or to make it less (or in some cases more) severe, or to make recovery easier by training and certifying pilots.

Despite all efforts to reduce stall and deep stall to acceptable levels of occurrence, such events still happen occasionally in the commercial aviation community, raising concern about their emerging complexity, dynamics and impact on public perception on safety of aviation (Salmon, Walker and Stanton, 2016). Such events have been subjected to major accident investigations are swerve as triggers for change throughout the industry. Most recent cases are Turkish Airlines flight TK1951, Colgan Air flight 3407, Air France flight AF 447, Air Asia flight 8501 and Air Algerie flight 5017. In a debate on high-altitude upset recovery, Sullenberger –captain of the Hudson ditching of flight US 1549- described stall as a seminal accident. "We need to look at it from a systems approach, a human/technology system that has to work together. This involves aircraft design and certification, training and human factors. If you look at the human factors alone, then you're missing half or two-thirds of the total system failure..."

A further analysis reveals some more fundamental flight performance issues (Obert, 2009):

- All stall recognizing and mitigating strategies have not eliminated the stall as a phenomenon; major stall related accident still occur.
- Airspeed indications rely on the use of Pitot tube technology. Applications of a new technology such as GPS provides redundancy in air data information.
- In contrast with roll and yaw control, pitch control of aircraft is not redundant. There are no substitute strategies for controlling pitch of commercial aircraft, in contrast with the military, where thrust vectoring is an option.
- Angle of Attack in commercial aviation is a secondary parameter, derived from Indicated Air Speed. There is no direct alpha indicator, in contrast with the military.

- 4th generation civil aviation aircraft lack the ability to create a negative pitch moment throughout the flight performance envelope by having direct access to speed and attitude as safety critical flight parameters.

While more pragmatic solutions have achieved a high level of sophistication in stall mitigation and recovery, a more fundamental approach to stall avoidance should be developed in order to deal with this intrinsic system property. An innovative solution to this more fundamental issue should comply with principles of dynamic flight control over the fundamental forces that are exercised on general aviation and commercial aircraft. This innovation consists of:

- Introducing new aerodynamic forces instead of manipulating existing forces;
- Introduction of such aerodynamic forces in uncorrupted air flow;
- Generating high pitching moments by small forces combined with long arms;
- Introducing correcting forces only in case of emergency.

An innovative design is suggested, based on these principles of dynamic vehicle control (De Kroes, 2012). Such a design is called a ‘stall shield device’, aiming at creating redundancy for lift generation during high Angle of Attack (AoA) conditions, supported by dedicated software and a flight simulator program. Assessment of the stall shield as a feasible and desirable innovation can only be done in the early phases of conceptual design on a consensus base. Discussing the issue of stall and remedies for stall related accidents cannot be allocated to a single actor or isolated contributing factor. Feedback from operationally experienced people such as pilots and accident investigators provide insights in the actual responses of the system under specific conditions that cannot be covered by an encompassing proactive survey during design and development. A multi-actor assessment should identify strengths and weaknesses, opportunities and threats of the stall shield, providing a safety impact assessment before the concept is released for practical use (Stoop and De Kroes, 2012)

5. Discussion

In accordance with such new conceptual thinking in complex and dynamic systems, systems states should be identified, either stable, quasi stable or unstable, inherent safe or unsafe. While safe and stable system states assess safety a non-critical value, inherent unsafe and unstable systems identify safety as a critical design and operational value, which permanently has to be designed, managed and controlled carefully during daily operations to avert disaster. Otherwise, the intrinsic hazards and inherent properties of such systems manifest themselves as emergent properties in practice. Providing transparency over the actual systems behaviour becomes pivotal in such critical and unsafe systems.

Complexity then can be defined as the interdependences of variables, choices and design assumptions. To deal with this complexity, it is not sufficient to decompose a system or event into its contributing variables and explanatory variables within its existing operating envelope and solution space. To identify and control change in the system and its dynamics, also the

design and change variables must be identified in order to serve as input for the engineering design process with respect to innovation and adaptation to meet new requirements. Across the various life cycle phases, stakeholders have a different safety perception, change potential and perspective on system change. While designers and engineers act from a socio-technical perspective during the design, management and governance will have their influence on socio-organizational issues from a control perspective. Operators and investigators derive their experience and expertise from operational practices, dealing with actual dilemmas and challenges from a naturalistic perspective.

In addition, dealing with complexity and context is not adding more detail and levels to an event by increasing the decomposition, but providing transparency at higher systems levels with respect to its functioning and primary processes, clarification of the conceptual properties, its configuration and composition. Complexity and dynamics deal with values, goals and motives and respond to unanticipated system transitions. A methodological question is how to establish the feedback loop between operational practices and engineering design from a socio-technological or socio-organizational perspective:

- Can we apply notions derived from systems value engineering, state/space modelling and chaos and complexity theory?
- Do systems engineering design methodologies such as simulation and prototyping provide an answer during assessment, testing and certification?

5.1 Value engineering

Value Driven Design (VDD) is a methodology which promotes the use of a more complete value function as the objective function to be solved through optimisation, rather than using a more limited formulation typically related to some performance metric or through managing the process of meeting requirements. However, this principle can be extended to consider not only the value of today's basic economic drivers but also to incorporate the ultimate value for the customer and even society, depending on who is implementing the Value Operations Methodology (VOM) that focuses on the ultimate value realised in through-life operation. Consequently, it is extremely well aligned to the problem of how to incorporate safety analysis into engineering and policy making decisions in their earliest phases. This has been incorporated into the fundamental VOM hypothesis as follows (Stoop and Van den Burg, 2012):

'the true value of an engineering solution is subjective, temporal and of an inherently transient nature, and therefore engineering value analysis and optimisation is more meaningful if formulated as the evaluator's preference for one state over another as a function of the quantitative difference in a number of key value levers related to the operational realisation of the intrinsic value of the product, process or service being considered.'

Consequently, safety is significantly elevated from the very basic consideration of factor, to a new level where it is being quantified as a multi-dimensional quantity with a resulting orientation that defines the choice of the designer or operator relative to their values

regarding safety. With reference to the Value Operations Methodology this leads us to the position where safety can be integrated into the general design approach of the air transport system together with cost efficiency, utilization, maintainability, environmental quality, and passenger satisfaction. Consequently, safety as a function of context, culture, content, structure and time can be characterised with the individual drivers associated with each dimension so that safety in its vectorial and most realistic form can be integrated into the overall integrated system of systems design solution space.

5.2 Simulation and prototyping: the ultimate load case

In making the transition from a linear safety intervention towards a dynamic safety intervention, the concept of critical load is applied. Accident scenarios can be considered critical loads on a system: once the critical load is applied, the system will fail if the load is increased, exceeding the load capacity under the given operational conditions and acceptable operator variability. For exploratory work on vectorial connotations of sociotechnical failure in aviation, references are made to by Chatzimichaillidou and Dokas (2015).

Complex systems modelling takes the form of representation by system state vectors, expressed by five primary systems dimensions –culture, structure, contents, context and time-, each with their own characteristic attributes, key performance indicators and metric values. Similar to such a system state vector, an event vector is identified expressed by its own characteristics such as hazards, actors, factors, aspects, causal relations, operating variance, interactions and operating conditions (Figure 1).

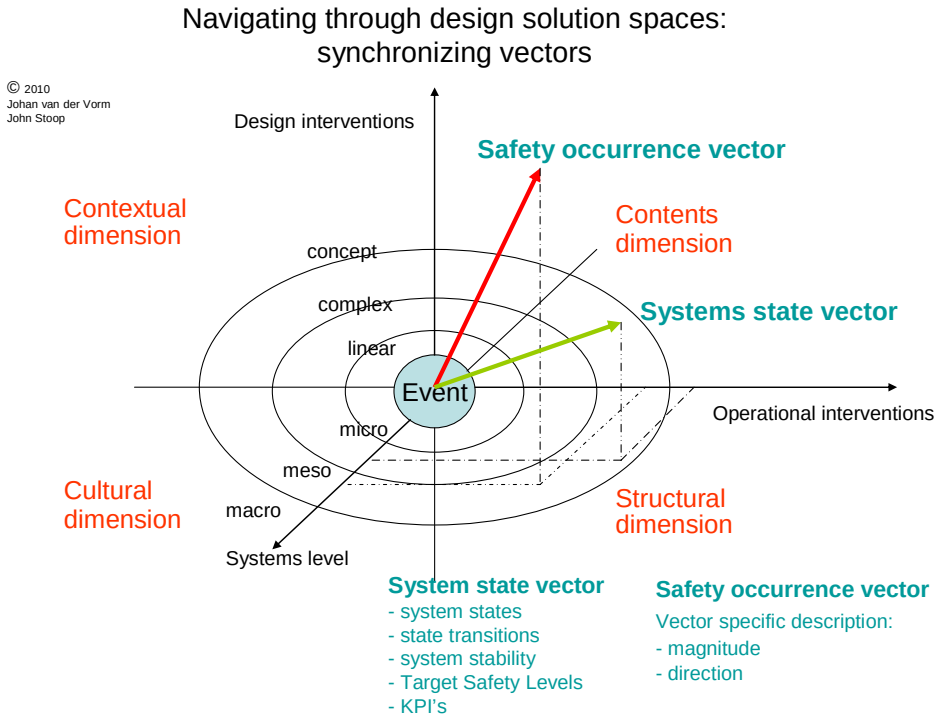

Figure 1. Multi-vectorial safety design solution spaces (Stoop and Van den Burg, 2012)

Navigating such an event vector through the systems operating envelope indicates proximity to operating limits and state transitions and consequently, a potential drift into failure. The challenge in optimizing safe solutions is the synchronization of these two vectors by transforming the event vector problem space into systems vector solution spaces within the boundaries of the available engineering design solution space. Such synchronization requires transparency over the various system state transitions, as well as a consequence assessment of the residual risk and side effects that remains after a transition.

In order to facilitate such synchronization, the Eigen Values of the event vector and system vector should be established to avoid oscillation and resonance. Analysing the potential systems responses is supported by testing the solutions in a virtual design environment by simulation and serious gaming techniques before the changes are implemented in the real world. By exposing the redesigned systems to the original ultimate load –the event scenario- the support for safety enhancement in terms of commitment for change, acceptance of the residual risk and feasibility for engineering design improvements are tested and validated.

In particular, for navigating the safety vectors through a value landscape, stability of system state basins and vector connotation are appropriate in answering questions such as; where are we, where do we want to go, how to get from problem spaces to solution spaces. Managing the required change by informed decision making can be supported by the shift from a causal factor notion towards a value vector notion (Stoop and Van den Burg, 2012). Eventually, optima can be represented by the use of multi-dimensional optimization surfaces such as available through Multi-Disciplinary Optimization software applications.

6. Conclusion

Safety is an intrinsic system value in the design optimization process towards preferential system states. Safety manifests itself as a system property throughout all phases of the life cycle in a specific form in all system states as either an intrinsic, inherent or emergent phenomenon. Although the notion of safety vectoring is still in its early phases of development, it contains challenges with respect to its operational validity and practical applicability in complex and dynamic systems. It provides a theoretical basis for establishing a working relation between design and operations by closing the feedback loop between the phases of the life cycle and system states. It may bridge the gap between technological and organizational perspectives in dealing with high energy density socio-technical systems. In such system vectoring, the notions of intrinsic technological hazards and inherent safety properties can be integrated in an overall system safety assessment before catastrophic consequences manifest themselves as emergent properties in reality.

References

Algemene Rekenkamer (2007). Risicobeheersing HSL-Zuid. *Kamerstukken II 31072*, nr. 1-2. (In Dutch)

Algemene Rekenkamer (2014). Hogesnelheidslijn-Zuid: Een rapportage in beeld.

Kamerstukken II, 22026, nr. 462. (In Dutch)

Apon J.P. (2016). Flexible Use of Airspace. Dutch Aviation Group, *Amsterdam Seminar, 26 Sept 2016*

Avionics Magazine (2016). SAAB to Bring Open Architecture to Civil Cockpits. *Avionics Magazine, 07-13-2016*

Chatzimicaillidou M.M. and Dokas I,M. (2015). The Risk Situation Awareness Provision Capability and its degradation in the Uberlingen Accident over Time. *Procedia Engineering, 128, pp 44-53*

Duivesteijn, A., Aptroot, C., Hermans, M.J.L.M., Koopmans, G.P.J., Slob, A. and Kool, V.M. (2004). Rapport van de Tijdelijke Commissie Infrastructuurprojecten [Report of the Temporary Commission Infrastructure projects]. *Kamerstukken II* 2004/05 29 283, no. 6. (In Dutch)

Eurocontrol (2010). Scan TF Supporting Regulatory tasks with Safety Scanning. The link between Safety Fundamentals, Safety Oversight Tasks and Legislation. *Eurocontrol Edition 0.9, working draft, 11 March 2010.*

Minsky H. (1986). *Stabilizing an Unstable Economy.* McGraw-Hill Publishers

Obert E. (2009). *Aerodynamic Design of Transport Aircraft*. IOS Press 2009 ISBN 978-1-58603-970-7

Offermans H. (2016). *Functional Airspace Blocks.* Dutch Aviation Group, Amsterdam Seminar, 26 Sept 2016

De Kroes J.L. (2012). *Commercial plane or flight simulator, adjustable fuselage control surface, computer program product and method.* Patent P96519NL0, deposited on 10 Jan 2012

Salmon, P.M., Walker, G.H. and Stanton, N.A. (2016). Pilot error versus socio-technical systems failure: a distributed situation awareness analysis of Air France 447. *Theoretical Issues in Ergonomic Science, 17 (1), pp 64-79*

Stoop, J.A., Baggen, J.H., J.L. Kroes, J.L. de and Vrancken, J.L.M. (2007). HSL beveiligingssysteem ERTMS: Een onafhankelijk naar nut en noodzaak van de aanpassing van het HSL-beveiligingssysteem ERTMS. *Rapport in opdracht van het onderzoeks- en verificatiebureau van Tweede Kamer der Staten-Generaal. Delft, Technische Universiteit. (In Dutch)*

Stoop J.A. and De Kroes J.L. (2012). *Stall shield devices, an innovative approach to stall prevention?* Proceedings of the Third International Air Transport and Operations Symposium 2012. Delft, 18-20 June 2012. Ed. R. Curran, Delft University of Technology.

Stoop J.A. and Van der Burg R. (2012). *From factor to vector, a systems engineering design perspective on safety.* PSAM 11 and ESREL 2012 Conference on Probabilistic Safety Assessment June 25-29, Helsinki, Finland

Toorenburg, M.M. van, Gerven, H.P.J. van, Elias, T.M.C., Vos, M.L. and Bergkamp, V.A. (2014). De reiziger in de kou: Rapport van de Parlementaire Enquetecommissie Fyra. *Kamerstukken II, 33678, nr. 11*. (In Dutch)

Van Kleef E. and Stoop J.A. (2016). *Life cycle analysis of an infrastructural project.* 51th ESReDA Seminar on maintenance and Life Cycle Assessment of Structures and Industrial Systems, 20-21 October, Clermont-Ferrand France

Walta, W. (2013). *The FYRA, a European Drama*. Personal communication.

Copyright Disclaimer