RESILIENCE FOR ENGINEERS

John Stoop
Kindunos Safety Consultancy, Spijksedijk 8A, 4207GN Gorinchem, the Netherlands
stoop@kindunos.nl ++31183637484

Abstract

This contribution elaborates on the need to integrate resilience capabilities from the start on into the design of socio-technical systems. Due to their ability to create catastrophic consequences, high energy density systems -such as aviation and railways- should not be measured by the absence or emergence of major events, but by their inherent properties, intrinsic hazards and recovery and resilience capabilities after major events. This contribution advocates the application of systems engineering principles and the revaluation of Good Airmanship as indispensable capabilities to engineer resilience in modern transport systems during design and operations.

1 INTRODUCTION

1.1 A shift in focus

During the last decade a paradigm shift has been observed in managing and controlling safety at both an operational, corporate and governance level from compliance with regulations to competence and continuous improvement of operational excellence (Stoop, De Kroes and Hale 2017).
First, underlying notions of operator's mental models are shifting from a Tayloristic focus on extrinsic motivation, productivity and command/ control strategies of their safety performance towards continual improvement, learning, adaptivity, quality and intrinsic motivation. There is also a shift from a focus on the individual operator and controlling risks to understanding underlying accident causation and systems dynamics on organisational and governance levels.

Second, due to a series of major accidents in high tech industries –internationally in aviation, maritime, railways, process and nuclear power supply- and emergent safety deficiencies in the design and development of major infrastructural projects –in particular in the Dutch railway industry- the focus is no longer solely on the operational phase. A shift is taking place towards design and handling of non-normal situations, aiming at knowledgeable interventions as well as the relative autonomous role of technological development and its interrelations with conceptual change and technological innovation, aiming at the requirements for adaptation at organisational and governance levels.

Third, as a consequence -rather than a static, linear modelling of events and concepts of systems architecture-, a shift in focus occurs towards systems modelling dealing with safe operating states/space models, system viability and recovery, survivability by the ability to respond resiliently to disruptive perturbations. Analysis is shifting towards interactions between external constraints and the configuration and geometry of complex systems throughout their states and phases.

From a systems design perspective, a shift occurs from the performance of the system's components to the performance of the whole system, to oscillation and stability of the Eigenvectors of systems, defining their survivability. Such shifting requires reflection on units of analysis and beyond that, the need to achieve synthesis between components, functions, and values. This is a major engineering design challenge. Current design strategies do no longer suffice at the level of options and opportunities derivate from regular performance, but require disruptive change, technological innovation and adaptation of underlying concepts and notions.

1.2 Resilience engineering

After a period of defining resilience engineering as a concept, identification and analysis of their inherent properties, questions are answered about why resilience is needed and what resilience engineering means in coping with complexity, adaptivity and systems dynamics. A need is emerging to achieve synthesis between contributing disciplines, generalization across application domains in order to make the next step to *how* to enact change, *how* to adapt and innovate in practice based on resilience principles. Such a need is particularly important for change in legacy systems with a global span of control on their networks, markets and social acceptance, in particular high tech industries in the transport domain.

2 CRITICAL TOPICS

Topics that proved to be critical in incorporating resilience in aviation, railways and infrastructure dealt with current engineering design principle in a series of major transport and infrastructural projects in the Netherlands. These systems are a distinct category of systems, due to their specific technological nature of high energy density systems and their legacy as long lasting entities.

2.1 Emergent criticalities

Emergent criticalities manifested themselves as:

- Transition strategies for deploying technological innovation and cyclic adaptation in the design and development of Schiphol Airport as a major infrastructural hub and implementing ERTMS on the Dutch railway network without serious disturbances or fatal errors in vital subsystems of the command and control systems during the transition period (Beukenkamp 2016)
- The use of survivability as a quantitative measure for resilience in the design and development of in particular the High Speed Line network development in the Netherlands
- Enabling a transition from the human error concept of pilotage to pilotage as a human asset for the design and operations of the 5th generation of commercial aircraft by introduction of Good Airmanship 2nd generation (Mohrmann, Lemmers and Stoop 2015)
- Identification and analysis of intrinsic hazards and inherent properties of high energy density technological systems as a specific category of complex and dynamic socio-technical systems.

These topics aims at:

- cross domain generalization of experiences with engineering resilience in a particular sensitive sector: legacy systems with a global, open network nature, combining a layered structure of a multi-actor involvement in the command and control of such systems and technological components at an innovative level
- development of system control theoretical concepts and models to pro-actively assess the safety of complex systems, both in their adaptive phase to major changes in technology, organisation and governance in early phases of design and development of new disruptive technologies, business models and market conditions.

Due to their already non-plus ultra-safe performance and expectations of a public confidence and risk acceptance nature, such systems require a dedicated design and engineering methodology with quantifiable safety requirements and performance indicators at a systemic level. Such design and development requires an upgrading of the man-machine interface from an either/or level towards a higher unit of integrated M-M-I analysis, combined with constraints of both external and internal natures.

The approach is based on combining concepts of control theory, systems engineering, resilience engineering and safety investigation. The approach has potential for design and development of new technologies, in particular in the transport domain.

2.2 Inherent properties

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, this 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. This 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.

3 SOCIO-TECHNICAL SYSTEMS BY DESIGN

Socio-technical systems must first and foremost be safeguarded by design due to their specific characteristics as a distinct category of high energy density complex systems. From a social perspective there is a conscious and multi-actor involvement in the optimization of conflicting values, goals and primary production processes. From a technical perspective, they may result in unacceptable catastrophic physical consequences by an instantaneous, unanticipated and uncontrolled release of high levels of energy of a mechanical, chemical or nuclear nature. They adapt to change in their operating environment by deliberate, disruptive and innovative changes in technology, organisation and governance. A proactive assessment of their safety performance is imperative to prevent unacceptable emergent behaviour and catastrophic consequences. The management of the total energy that is stored in the system is a challenge that must be controlled proactively throughout all system states, mission phases and operating constraints.

3.1 High energy density systems

Due to the increase in size and scale of modern socio-technical systems, the uncontrolled release of energy can result in catastrophic material consequences and loss of all lives of a large population at risk, both inside and outside a system. The total energy stored in complex systems can be expressed in Megawatts as the sum of its kinetic and potential energy. The energy content of a High Speed Train and a Jumbo jet can be compared to a nuclear power plant, as depicted in table 1.

	weight	speed	altitude	Energy/sec
High Speed Train	430 tons	250 km/h	ground level	1053 MW
		320 km/h	ground level	1740 MW
A380 Jumbo jet	MTW 575	900 km/h	10.000 m	75 000 MW
	at take-off MTOW 575 tons	260 km/h	ground level	1500 MW
	at landing MLW 386 tons	260 km/h	200m above ground level	1252 MW
Nuclear power plant	Average size			800 MW
	Borsele (Neth)		Sea level	450 MW
	Chernobyl		Sea level	600 MW
	Fukushima		Sea level	784 MW

Table 1 Total system energy content

Such a total energy management strategy is interesting in particular in aviation with respect to the balance between kinetic energy due to the airspeed control and potential energy due to the altitude and attitude control. The total energy of an aircraft has to be controlled and dissipated back to zero in order to bring the flight to a safe end. This kinetic and potential energy distribution varies across the various flight phases. The total energy of an Airbus A380 in cruise flight is about 75000MW. This amount of energy is the sum of 18700 MW of the airspeed (Mach 0.85) and 56400MW due to the cruising altitude of about 11000m. This means that the energy balance management in this flight phase is based for 25% on the speed control and 75% on the altitude and attitude control. During landing, the kinetic energy reduces to 1006 MW at 260 km/h minimal

landing speed at Maximum Landing Weight MLW of 386000 kg and the potential energy to 246 MW at the Maximum Landing Weight at 200 feet over ground level, the go-around decision height. The total energy during landing is about 1252 MW. The potential energy at 200 feet altitude in final approach is reduced from 75% at cruising altitude to 19.6% of the total energy content. The energy ratio management changes towards a predominant control over speed and attitude.

3.2 Multiple performance indicators

Historically, safety in aviation is not only expressed in achievements and policy targets but also in technical airworthiness requirements. Taking into account that zero risk is unachievable in any human activity, acceptable safety target levels had to be established in the perspective of an unbalance between safety and expected growth (Hengst, Smit and Stoop 1998). An array of potential units for measuring risk can be used, discriminating *relative* safety related to the traffic volume and *absolute* safety, related to the annual number of fatalities. Differences across fleet segments and services, scheduled, non-scheduled flights and general aviation, accident rates per aircraft class and world region, as well as life expectancy of aircraft have to be taken into account because risk acceptance by the general public and personal appreciation of risk depends on convenience and pleasure in the various types of private and public risk taking activities. For each activity, a unit of measurement has to be selected since it makes a large difference whether safety is related to the absolute number of fatalities, a critical flight phase or the distance and time flown. For *air services*, as the criterion for safety performance the fatality rate per passenger km is used, while for *airworthiness* the level of safety is expressed per aircraft hour of flight. These two criteria are related by the number of passengers per aircraft, the survivability rate per aircraft and the blockspeed of the aircraft (Wittenberg 1979):

- Number of passengers km P
- Aircraft flying hours U
- Aircraft flying kilometres S
- Assuming K passenger fatalities in R fatal accidents, the fatality rate per passenger km is K/P and the fatal accident rate per flight hour R/U.

For the relation between these quantities holds:

Eq (1) $K/P = R/U*K/R*U/P$

In this expression are introduced:

$k = K/R$ = average number of fatalities per fatal accident

$p = P/S$ = average number of passengers per aircraft

$V_B = S/U$ = average block speed

Then for equation (1) can be written:

Eq (2) $K/P=R/U*k/p*1/V_B$

Or in words: Pass.fatalities/pass.km = fatal acc./flight hours *fatal per acc./pass per aircraft*1/blockspeed. This dimension analysis shows that the introduction of long haul flights, increased survivability rate per accident, increase in blockspeed and larger aircraft have had a major influence on the decrease of the fatality rate per passenger km.

In addressing the issue of acceptable safety levels, two assumptions were made:

- With the expected increase of traffic volume, safety levels may not fall below the achieved levels for reasons of public acceptance
- The level of growth is linear related to the number of accidents.

In socio-technical systems with a high safety performance level, such as aviation and railways, these assumptions proved to be obsolete due to the non-linearity of complex systems and changes in public safety perception and appreciation.

3.3 Changes in system performance indicators

Business models and earning systems as incentives for efficiency versus thoroughness trade-offs are very powerful drivers for cost-efficient operations. In modern business concepts, calls for lean production, faster, cheaper and better performance are frequently heard.

With the introduction of New Economy principles in the transportation sector, three simultaneous developments have changed the drivers for cost-effective decision making. Changes in economic and logistic

infrastructures, safety philosophy and selection mechanisms for preferential solutions have shifted from safety performance criteria towards exploitation, availability and cost-efficiency criteria. Cost-benefit considerations and environmental constraints in operations have become dominant. Instead of covering technical deficiencies by an array of technical provisions, a 'willingness to pay' and cost-effectiveness of solutions have become prevalent. Other arguments than safety have to been taken into account in decision making.

Differences in expertise are considered hindrances or even unjustifiable instruments to control the outcomes of a consensus process. Such an environment of 'participative policy making', assumes equality between parties and change the role of experts. Public private partnerships are favored as an answer to hierarchical ordered governmental projects on major infrastructural projects in tunneling, railways and aviation. Safety becomes a 'social construct' instead of an outcome of objective assessment based on professional experiences, quantifiable performance parameters and expert opinion. Such a 'new approach' in safety thinking shifts the focus towards prevention, flexibility, cost-benefit considerations , quantification of key performance indicators and institutional arrangements. This 'new' approach is a response to the inadequacy to provide substantive progress in conventional safety in the context of a 'new economy' context. Implicit assumptions are that the market should be best prepared to bear the risks and supply the knowledge, while a process approach should drive out substantive approaches. Private parties should not be disturbed by approval of their technical solutions, but should have their hands free to inform government about their selection of preferential solutions. Performance of a systems is reduced to measurable and quantifiable performance indicators. Safety is not such a parameter. Such a regime may reduce or improve the overall safety performance level of a system.

In comparing similar concepts, two options emerge:

- a low systems safety level, characterized as a earning system. In such a system, liability issues, blame and performance are pivotal. Willingness to pay and ALARA techniques prevail, while rule compliance and inspections are important control mechanisms. Safety is controlled at the organizational and company level.
- a high systems safety level, characterized as a learning system. Such a level is guaranteed by quality performance, transparency, communication and cooperation. Sharing responsibilities and information is essential for common learning and indirect cost are recognized. Responsibilities and roles are guaranteed by institutional arrangements.

In selecting either of such options as preferential, specific criteria should be available. Identifying systemic values in a multi-agent based environment has become a topic.

4 Prerequisites for engineering resilience

4.1 Towards a systems engineering perspective

The percentage of the total growth of the traffic volume expressed in passenger km must be compensated by an equivalent decrease in percentage of the fatality rate per passenger km. In the past, safety improvements have been accomplished pragmatically changes in technology, aircraft operations and ground equipment. These achievements have been a combined effort of all parties involved: manufacturers, airline operators, authorities and research institutes.
Advocating a more rational tool for establishing a safety level -such as cost-benefit analysis- such approaches are confronted with hardly comparable costs for value of life, operating costs and cost for safety investments. While costs of individual accident are relative low on a sectoral level of costs, the overall safety enhancement measures following from such accidents may be excessive for the sector. A target safety level for aviation based on a rational cost-benefits approach seems hardly achievable (Wittenberg 1979).

Consequently, another approach has to be favoured where likely improvements can be obtained: the analysis of aircraft accidents and the identification of their causes. A distinction is made in two principal categories in this analysis of aircraft accidents: accidents occurring during normal flight conditions, attributable to a lack of airworthiness and operational factors, and accidents during non-normal flight conditions such as due to human factors, either flight crew, ground personnel or weather conditions such as turbulence. Historically, two practical, operational areas for improving air safety have been applied (Wittenberg 1979):

- The human factor. The predominant position of the human factor as an accident cause only partly can be contributed to direct fault in the performance of the flight crew. The human error is compounded by deficiencies in the design due to a lack of human engineering or by inadequate training for the job to be performed.

- Classification of events by primary production functions, flight phases and system states. Improvements of equipment and procedures for aircraft navigation and air space control will be required to cope with the increase of air traffic in the future. Areas with already dense traffic flow - in particular in the Terminal Movement Area- will benefit from congestion and conflict handling measures.

More rational approaches had to be developed in the 1970's for the introduction of civil jet aircraft and new technologies such as the supersonic Concorde and Automated Landing System development. The allowable probability of failures is inversely related to their degree of hazard to the safety of the flight. No single failure or combination of failures should result in a Catastrophic Effect, unless the probability can be considered as Extremely Improbable, in effect lower than 10^{-7}. Interesting in this approach is the total amount of flight hours per year that are produced by the aviation industry as such. Only a few aircraft types can surmount the 10^{7} requirement, accumulating sufficient flying hours. Consequently, accomplishment to the overall safety target of the airworthiness code *can never be proved by actual flight data* but should be settled by a System Safety Assessment approach. Due to the effect of the increase of aircraft speed and aircraft size, the passenger fatality rate expressed per passenger km has decreased in the past far more than the fatal aircraft accident rate per flight hour. In the coming decades, the favourable effect of increasing aircraft speed and increasing aircraft size will no longer occur. This parameter analysis demonstrates that changes in aircraft size and long range flights had an impact on the improvement factor required for the fatality rate per *passenger km* versus the fatal accident rate based on the *aircraft flying hours.* Consequently the adoption of this new rationalized safety approach severed the assumption of a linear relation between accident rates and traffic growth. As a consequence of the return to smaller aircraft after the jumbo jet era and the very high survivability rate, a shift in safety focus occurs from aircraft design parameters to operational parameters and other primary system components; airports and ATC.

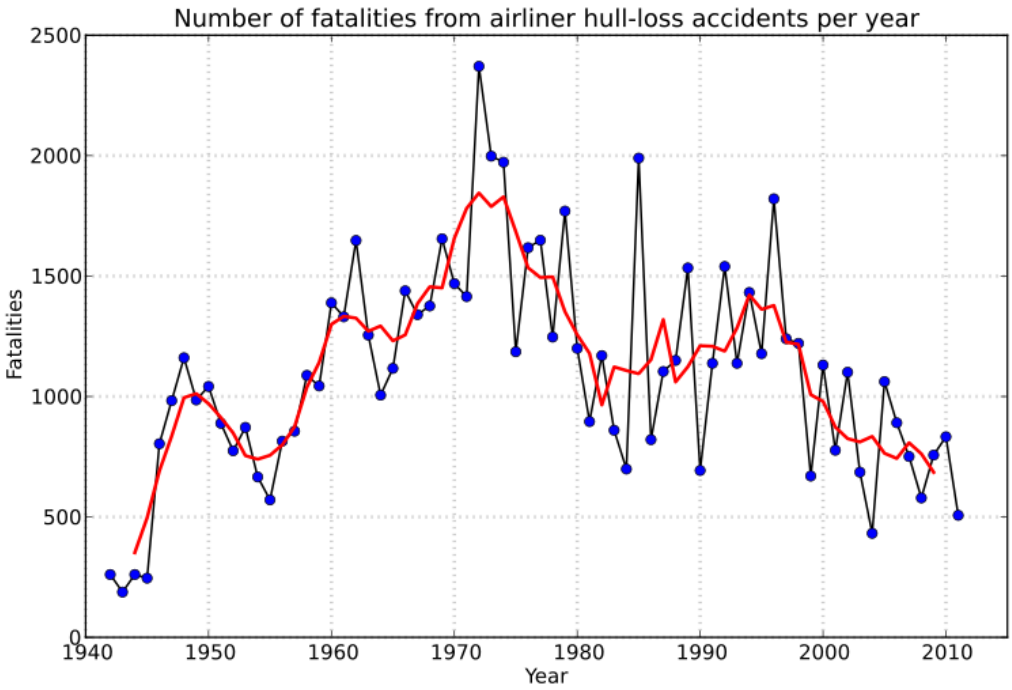

Fig 1 Non-linearity between safety performance and growth

The FAST (Future Aviation Safety Team) and CAST (Commercial Aviation Safety Team) projects in the EU and USA serve to improve the aviation safety level in passengers fatalities per passenger km, to compensate the increase of the transport volume in passenger km of the 1990's (FAST 2014). Simultaneously, the introduction of glass cockpits, pilot information processing and decision making support systems and satellite support facilities for flight crews and ATC each have had their share in the safety enhancement of commercial aviation. A transition to a safety assessment of the overall aviation system is under way: focusing equivalently on the three main components aircraft, airport ant ATC throughout their operational processes. The architecture of systems becomes a focal point of concern.

4.2 Towards a systems architecture

By identifying four dimensions of a system, a problem can be approached from different viewpoints by making

a number of 'cross sections' through a problem. If these cross sections are properly chosen, each cross section shows different 'dimensions' of the problem. Such a structured search is referred to as the 'dimensions' technique (Stoop 1990). The objective of the 'dimensions' technique is to establish a description of the problem in the context of a socio-technical system which makes a reference to the life-cycle, dynamics and structure, culture, context and content the relevant system dimensions.
The 'dimensions' are respectively:

- historical: this dimension provides insight into the development of the problem and the long-term development of its technical, organizational and social factors and hence, of the controllability of the problem in the context of the long term development of the system. This dimension covers the Context of a system
- life-cycle: from design, development, manufacturing, through us towards demolition. This dimension gives insight into the feed-forward and feed-back coupling of knowledge and expertise between system phases and knowledge about the criteria relevant for improvement and change. This dimension covers the Structure of a system
- process: this dimension gives insight into the 'normal' use of the system and describes the content of the processes that occur in 'normal' functioning. It gives insight into the tasks, activities, procedures, tools, equipment, operating environment, inputs and outputs of the system. This dimension covers the Content of a system
- culture: this dimension characterizes the system as occupational, transport. leisure or domestic. It gives insight into the (social) objectives, of the system, the role, positioning and functioning of stakeholders, their views, norms, values and codes of conduct. This dimension covers the Culture of a system.

The 'dimensions' technique collects data from normal as well as disturbed functioning, addressing all available performance indicators from intended and actual use and develops from broadly descriptive towards detailed explanatory. Data collection can be conducted by literature study, interviews, document analysis, on-site investigation and other forensic techniques.
The four dimensions are explored in parallel and should result in credible, plausible and verifiable description of the problem under scrutiny in its systemic environment.

4.3 A system life cycle approach: the DCP diagram

In order to integrate safety in design and operations, a new notion of vectoring safety through the systems landscape should be defined. Such a notion consists of three principal elements, being Design, Control and Practice (DCP). They can be interrelated along three dimensions, being a systems approach, a life cycle approach and a design approach. Together they constitute an integrated systems architecture prototype: the DCP diagram.

A systems dimension defines three levels: the micro level of the user/operator, the meso level of organization and operational control and the macro level of institutional conditions.

The life cycle dimension defines a series of subsequent phases, being design, development, construction, operation and modification. At this dimension, the coordination of decision making among actors across the phases is crucial.
The design dimension identifies three principal phases in design, being goal –expressed by a program of requirements, concepts and principles-, function –expressed by design alternatives- and form, expressed by detailed design complying with standards and norms. At this dimension, the potential of technical innovation for new safety solutions is crucial.
The operational dimension. Eventually, only in practice safety is visible and actual consequences of accidents occur. At each of the other levels and phases however, separated in time or space, safety critical decisions have been made by different actors. The diagram demonstrates who, how, at which moment can contribute to safety and risk assessment

To manage consequences of new technology and innovation in transport systems engineering design, three principal lines are available:

- the Practice-Control line. Along this line, an upgrading in interventions takes place. The focus shifts from the performance of individual operators towards the meso level of organization and management in allocating resources, skills, operating procedures and responsibilities. At a macro governance level, rules, regulations and legislation, inspection, certification and governance oversight are addressed as safety enhancement opportunities.
- the Design-Control line. Along this line, decision making and safety assessment methods and standards should be elaborated, to facilitate coordination among stakeholders and actors, participating in major

project developments. Several initiatives have already been taken such as safety impact assessment techniques, harmonization of standards by drafting EU Guidelines and Directives on specific topics such as tunnel safety, land use planning or external safety.

- the Design-Practice line. Engineering design methods for integration of safety in technological innovation are in their earliest phases of development. Historically, an impressive variety of design techniques is available. However, these instruments focus on specific industrial sectors and detailing levels of engineering design of components and are not always generically applicable across modes, disciplines or sectors.

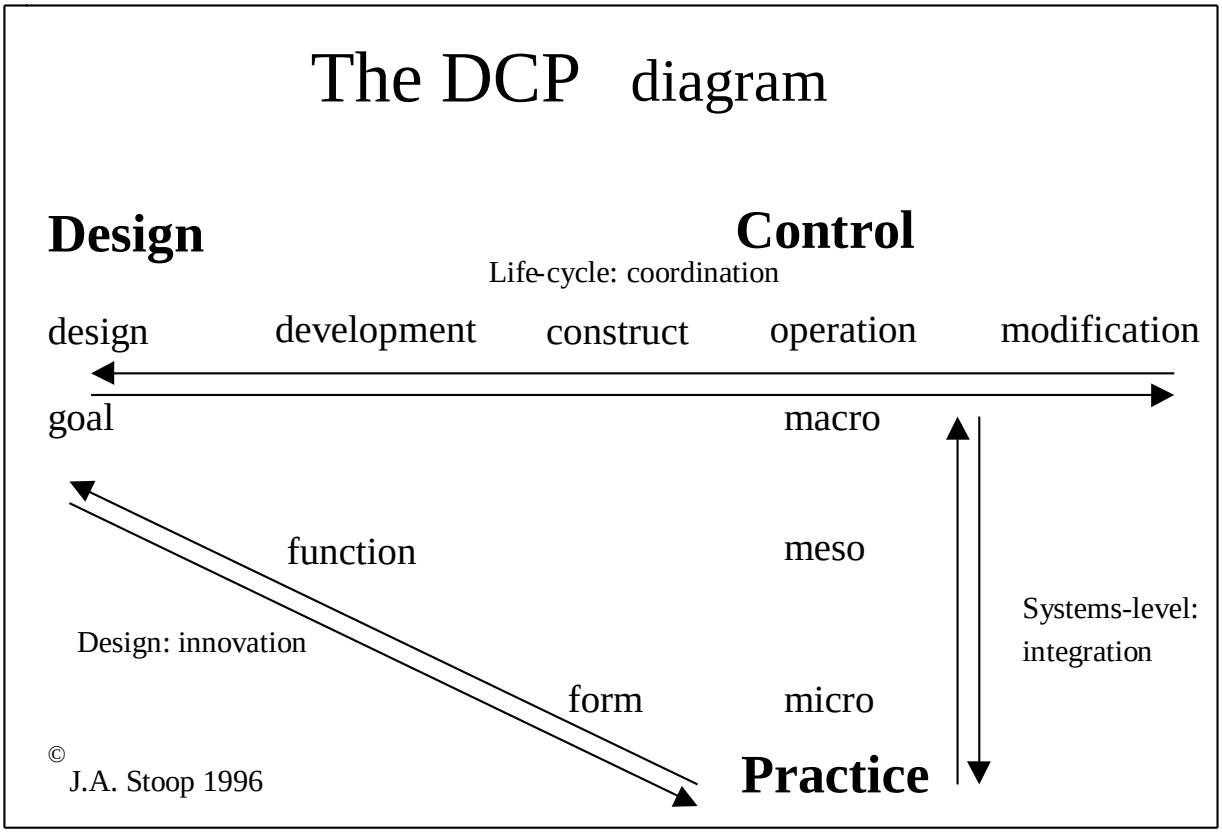

Fig 2 The Design, Control, Practice diagram

In order to design a coherent system and to maintain oversight over the system functioning, a system safety integrator role should be defined. During the design of complex transport systems, a dedicated responsibility should be allocated to assure continuous monitoring of the safety aspects along both lines during its design.

Abolishing obsolete safety constructs

To the purpose of a scientific safety analysis of recovery and resilience capabilities, it is inevitable to abolish three obsolete constructs that have dominated the debate on safety investigations:

- Probable cause, to be replaced by plausible scenario descriptions
- Human error, to be replaced by the notion of reasonability of responses
- Accident modelling, to be replaced by investigative event reconstruction.

The first two constructs have a history as judicial and psychological construct and are frequently criticized for their theoretical and practical applicability during investigations. Such criticisms are mainly based on experiences in the process and nuclear power industry as stationary and hierarchical organized and managed corporations and small and medium enterprises with simple and less complicated events. In major investigations in the transport industry -in particular in aviation and the maritime-, scenario descriptions and reasonable responses have a legacy in accident prevention and Good Airmanship/Good Seamanship.

The construct of reasonability of responses has a history in tort law and disciplinary law, in assessing professional conduct and ethics. This construct became disconnected from safety investigations with the introduction of blame free and preventive investigations and has to be re-introduced in the framework.

5 GOOD AIRMANSHIP

Towards a human habituated response

In cognitive modelling of pilot behaviour, the common reductionist paradigm is to deal with the pilot as a rational, knowledge based and informed decision maker. Many decisions and actions however are routine based, executed at the skill and rule based level of cognition. Such responses are trained, engrained and maintained by simulator training, recurrence and proficiency checks, line checks, incident reporting and audits. Decisions and actions however are not only rational. Since the research of Pavlov, the importance and impact of intuitive, emotional, conditioned and subconscious responses is recognized. Conditioned, automatic responses are predisposed responses based on expertise, competences and previous experiences. The rationalization of such decisions, actions, reasoning and motives remains speculative until after the actions. In general, operators trust on their experiences with similar problems. Their trust and experience will lead to 'automatically' right decisions and actions, compliant with expectations. The reasons for such performance can only be retrieved in hindsight by observations, interviews, recorded conversation and re-enactment of the action sequence. The role of intuition, instinct, reflexes, predisposition, beliefs and emotions is obscured until the actual outcome of the actions (Mohrmann, Lemmers and Stoop 2015).

In analysing a series of accidents, Den Hertog and Roelen (Den Hertog 2011) posed the question why well trained and experienced pilots with high qualifications could fall into a trap of formally incorrect responses to emergent safety issues.

They clarified a recurrent chain of events in which managing concomitant abnormalities and prioritization of event handling lead to the detriment of a safe flight performance, induced by the fact that they were primed due to prior events in their problem solving process.

Such a chain of events that becomes safety critical, contains a succession of an aircraft malfunction, an abnormal situation and unusual conjunction of conditions, decisions and actions that, if they were to occur individually, are relative benign. The accidents arose out of usual human performance in unusual circumstances (Den Hertog 2011).

The components of such a chain repeatedly consisted of:

- A technical malfunction which unanticipated interacted with other system components
- Creating multiple phenomena simultaneously of a relative benign nature
- While in a stressful situation, mutual reliance on crew competences in a professional environment
- Primed with problem solving of prior events
- Deprived the crew from recognition of the actual system state and situation.

In these accidents a combined occurrence of technical failure, automation surprise and flight performance collapse created an aerodynamic stall which became unrecoverable. Successful recovery in such situations does not rely on better training or enhanced flight deck design, but on the available time, resources, information, recovery options and regaining control over the situation. Such situations have been demonstrated to be survivable, even beyond expectations, by the A300 Bagdad missile attack, the US 1549 Hudson ditching and the Qantas A380 recovery to Changi Airport. In these situations, the ability to generate new options beyond regular trained situations contributed to the recovery of the situation.

In the analysis of habitual responses, the perspective of a conventional human performance analysis is abandoned. Instead of asking the question why the crew deviated from regular performance, the question is posed: why did their performance make sense to them at the time? A better understanding of human behaviour and decision making under stressful situations, unusual conditions and habitual responses can assist to improve flight training and flight deck design.

Such understanding requires the abolition of conventional notions because they proved to run short in providing a satisfactory explanation of the event and intervention in the situation:

- No proximate or remote cause was established
- No critical human error was identified as a satisfactory explanation of the event
- No accident models could have grasped the phenomenon with respect to the habituated responses that were identified in the investigation.

The debate on erroneous pilot responses to system malfunctioning frequently refers to situation awareness and automation complacency in complex socio-technical operating environments. The issue of habituated responses and successful recovery addresses a much wider range of operator's responses, irrespective of

technological complexity or transport sectors. It has a long history in the maritime, aviation and railway sectors.
In the early 1960's, the Dutch Railway Investigation Board introduced the issue of reasonability of responses formally in her working procedures in order to learn from the practical experiences and expertise of train drivers (De Kroes 1996). Board members had unrestricted access to train drivers -not only those involved in accidents- and were allowed to observe train drivers in their daily work and interview them accordingly after their trips. This made it possible to ask why it was reasonable for these operators to decide and act as they did. Such an approach provided a timely and direct access to train driver perceptions and decision making both in regular and safety critical conditions. This approach was later internationally published and made accessible for academics in a popularized version by Sidney Dekker in 2005 with his seminal book *Ten Questions about Human Error.*

6 CONCLUSIONS

Based on our experiences with major transport and infrastructure projects in the Netherlands, in this contribution we have identified a specific class of socio-technical systems: high energy density systems. To enable recovery and resilience in such systems, such capabilities should be designed into these systems as inherent properties.

Measuring the safety performance of such systems cannot be restricted to a fatality or injury rate as manifested during operations, but also should take into account characteristics of the primary processes-such as services provided and service worthiness- and economic drivers for change and their underlying business models. This requires a shift towards a system engineering from both a Design, Control and Practice perspective.

Finally, several dominant but obsolete safety constructs have to be abolished in order to facilitate a shift to integrating resilience into the design process at the system architecture level. To this purpose, in particular a shift from 'human error' to a habituated and intuitive Man-Machine-Interaction level is indispensable.

REFERENCES

Beukenkamp W., (2016). *Securing Safety*. Doctoral Thesis Delft University of Technology.

Dekker S., (2005). Ten questions on human error. Ashgate

De Kroes J.L., (1996). *Slachtoffers.* Valedictory Lecture, Delft University of Technology.

Den Hertog R., (2011). Two accidents analysed another way. 'Free will does not exist'. Future Aviation Safety Team presentation November 2011.

Hengst S., Smit K. and Stoop J., (1998). *Second World Congress on Safety of Transportation*. 18-20 February 1998, Delft University of Technology. Delft University Press

Mohrmann F., Lemmers A. and Stoop, J., (2015*) Investigating Flight crew recovery Capabilities Regarding System Failures in Highly Automated Fourth Generation Aircraft*. Aviation Psychology and Applied Human Factors 2015, Vol 5(2) pp . 71-82

Stoop J., De Kroes J. and Hale A., (2017). *Safety science, a founding fathers' retrospection*. Safety Science 94 (2017) 103-115

Wittenberg H. (1977). *Safety in aviation; achievements and targets*. Technische Hogeschool Delft, Lucht- en Ruimtevaarttechniek. Memorandum M-353