Eric A. van Kleef
Van Kleef Consultancy, Leusden, The Netherlands

John A. Stoop
Kindynos Veiligheidskundig Adviesbureau, Gorinchem, The Netherlands

Can we cast resilience in concrete?

Keywords

infrastructure, systems, adaptation, resilience

Abstract

Infrastructural systems -such as railways- can be characterized as multi-actor socio-technical systems that are able to adapt during their life cycle, both to external disturbances as well as changes in the system itself. The design phase should mark the starting point for a resilient system to prevent ad-hoc and opportunistic design changes. A case study on the design and development of the High-Speed Line railway system in the Netherlands indicates that it is necessary to make both a technical and procedural evaluation of these future user's possibilities before construction takes place. Once cast in concrete, the adaptive potential has been determined.
The actors during design and operation adapt in different ways. During the design, the focus should be on the question which incentives are driving the designing parties towards a consistent and resilient design. The task for a strategic engineer or architect, is to understand how incentives and requirements influence each other and how they safeguard the future operational variance of the system and its safe performance. Such a strategic engineer should be involved in the project at the functional level, where requirements and incentives are formulated.

1. Introduction

Infrastructural systems are multi-actor socio-technical systems. They do not only exist of technology, but are very dependent on humans as well. Socio-technical systems are not static. The human components vary their behavior and adapt to changes in their environment. Variation in human performance is often blamed for during accidents. This same variation, however, is the source of adaptation during design and development of the system, which in turn is an important aspect of resilience.
A system that only exists of technological components cannot adapt to changes. If the system's environment changes and the system remains unresponsive, the system will eventually break down, resulting in loss of performance or an accident. The technological components alone are not sufficient to guarantee resilience or safety. Also assigners, designers and decision makers should be resilient.

2. Adaptation

During the system's life cycle the system's environment changes. The technological components cannot adapt to these changes, but the human components can. The same variation that is often seen as 'human error' is the source of the possibility to adapt. This is one of the roots of resilience. The human components in the system always vary around some best practice. Humans copy behaviour, either from written prescribed procedures or from their own experience. Good variations from the viewpoint of the person involved, are selected and copied a next time. These small variations accumulate and make the behaviour drift away from the starting point.
Adaptation in systems bears a resemblance to evolution. It is an internal change of the system on a large time scale [5]. It can be considered an unintentional process that results from variation, knowledge dissemination and selection of good variations. It is unintentional in the sense that no a-priori direction of the adaptation is necessary for adaptation [9]. These adaptations are vital for the

survival of the system in changing environments. If the system cannot adapt to changes, it is not resilient. Woods calls this sustained adaptability [15]. The described way in which adaptation takes place has another consequence. Only adaptations are possible that have viable intermediate systems. Adaptation by small accumulating variation will take place almost unnoticed and can be the result of an autonomous process, while larger changes need redesign. In such a gradual assimilation process, three magnitudes of change can be identified: optimization of current operational performance and processes, adaptation by reallocation of functions and responsibilities, procedures and regulations, and innovation by conceptual change and application of new technologies [3].
During the design stage, adaptation is not restricted to the human and organizational components of the system; also the technological components change and adapt to a changing environment.

3. Design

System design aims at safe operation at the moment the system is taken into operation; the design stage marks the starting point for all future adaptations. In the design stage, the technological components and the initial organization and procedures are determined. At the same time, the possible future adaptations of the system are determined. Not every future adaptation can be reached from the designed starting point without redesign. The design stage is the only moment in a system's life cycle where the technological components can adapt too. Later on, the adaptation is restricted to the human and organizational components, while the technology remains relatively static. Consequently, the potential for a sustainable change is limited: Once cast in concrete, the adaptive potential has been fixed. The static parts of the infrastructure cannot adapt anymore and even worse cannot easily be changed. The physical, concrete components of the system have a lifetime of 50-100 years. Software components last for about 5 years with numerous versions and short-term upgrades. The more components are made technological and the less are human, the less the adaptive potential becomes. In order to get a resilient system that can adapt to future changes in the environment, it is necessary to make a thorough technical evaluation of future possibilities before construction takes place. A potential mismatch between hardware, software and life ware - each with their own life cycle- may create emergent properties and unforeseen interactions that may lead into disaster.

Structuring transport systems takes place by analyzing the dynamics between actors, factors and aspects, their interrelations and system components as they are configured at the various systems levels. To this purpose the TRAIL Layer Scheme has been developed [4]. Each layer in this Layer Scheme facilitates the next higher level by supplying a service, and in return, is governed by the decisions of these higher levels, while interactions with the environment are specified (figure 1). The Scheme provides transparency over market interactions, their supply and demand dynamics and decision-making constraints.

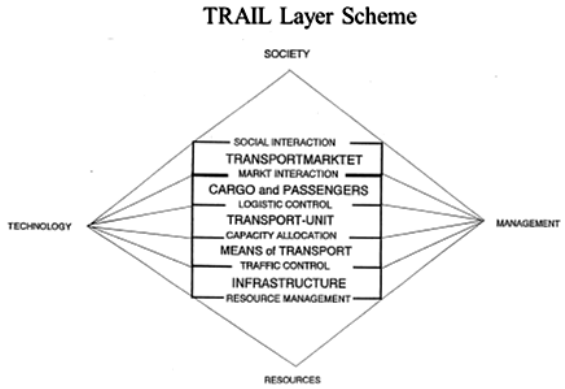

Figure 1. Structuring transport systems.

A chronological review of a major project in the Netherlands -the High Speed Line project over the period 1994-2015 illustrates how each of the major system components and layers was submitted during the design and construction to complexities in the decision making under conditions of unforeseen external influences. This complexity deals with both substantive issues in technical design as well as with procedural issues in decision-making strategies in a public-private partnership environment. Due to the national level of the project, at several points in the decision making process, political intervention by Parliament occurred, up to the level of two Parliamentary Hearings.

3.1. High Speed Line Business Model: A paradigm shift

The EU Directive 1975/327/EU on interoperability is considered a benchmark for opening up the European railway network. The goal is to create free transport of passengers and cargo and to establish a competitive rolling stock manufacturing market across the member states. It aims at an interoperable network with interchangeable, harmonized components [13]. Creating a competitive rolling stock manufacturing environment should terminate national railway monopolies with inherent obstructions for sharing infrastructure, signaling and

rolling stock between competitive operators. To this purpose a separation was created between infrastructure, service providers and operators. The development of an innovative, European signaling system ERTMS should enable a capacity increase on the new network. Simultaneously, ERTMS should facilitate interoperability and foreign competition on previously national networks by replacing national signaling systems. The Directive also changed the business model of the national railways in a fundamental manner. In the 19th century concession system a link existed between the number of passengers transported and the financial resources for investing in the railways. There was a direct link between financial earnings and expenses. In the new system, national governments have the obligation to provide public transport. A system of governmental subsidies became necessary to provide operators with sufficient capacity and availability of the infrastructure. This judicial business model caused staggering costs over the past two decades because the actual use of the capacity by operators became less relevant. To reduce the costs of providing high quality infrastructure, national governments have the incentive to transfer design and development costs to manufacturers. This business model discourages governmental involvement in technological teething troubles in ERTMS and rolling stock.

The EU Directive considers such technology as turnkey projects without involvement of governmental inspections or operators. The introduction of ERTMS offers a major incentive to transfer design development and operating costs of signaling systems from the infra provider to operators. Eventually, the ERTMS level 3 enables the government to become fully independent of all costs involved in implementing signaling system, because this ERTMS level 3 is a full on-board version with only minor infrastructural components. The concept of life cycle responsibilities is substantiated by Design, Build, Finance and Maintain contracts. Conventional design and development were a shared responsibility of commissioner and designer, with detailed product requirements, production instructions and daily supervision over the manufacturing process. The new concept does not apply national safety certification procedures and standards, but relies on certification, testing and exploitation requirements of independent Notified Bodies (NoBo's). Approval by independent NoBo's provides access for multiple operators with their own rolling stock on each of the national networks. To this purpose Technical Standards for Interoperability (TSI's) have been developed. To facilitate competition between the large national equipment and component manufacturers, such TSI's have been defined at the functional level. Consequently, each manufacturer has the flexibility to design equipment at the detailed level according to its own resources, capabilities and experience. Trouble shooting in case of deficiencies and teething troubles are dealt with without interference of national approval authorities or procedures. It is an exclusive manufacturers responsibility [13].

Effective protection of the network by national railway companies and national governments prevented achievement of the goals of the EU Directive. The introduction of the concept, however, has been successful for the High Speed Line projects, although not without troubles. In the Netherlands, two major technical problems had to be faced: the troublesome implementation of ETCS -the technical component of ERTMS- on the international HSL network with Belgium and the introduction of high speed rolling stock, -the Ansaldo Breda manufactured Fyra-. These problems occurred simultaneously but independently from each other.

In practice, several external influences intervened in the development process: tunnel fires in the Channel Tunnel and Alpine region impacted heavily on tunnel safety requirements, while the derailment of the ICE train at Eschede in 1998 created debates on appropriate measures for prevention of derailment accidents at high speeds. Several other events did not play a role during the design and development phase, but emerged in the first months of operations of the Fyra only years later on.

3.2. Design and construction of infrastructure

Between 1998 and 2009 a new high-speed rail connection was built from Amsterdam to Antwerp. The Dutch Ministry of Infrastructure and Transport made a preliminary design prior to commissioning the project. The civil structures were commissioned in seven parts to civil constructors; the tracks, traction and signaling were commissioned to an infrastructure provider, while the rolling stock and exploitation of the line were the responsibility of the railway company who got the concession to exploit the line [6]. The civil constructors got a design-and-construct contract, the infrastructure provider a design-build-finance-and-maintenance contract. The railway company had to pay for the concession to exploit the line. The civil contractors had to optimize their design on building costs; the infrastructure provider had severe performance requirements forcing them to optimize their building and maintenance costs. The railway company had to optimize on costs of rolling stock and exploitation. One of the hazards identified in the preliminary studies on the high-speed line was derailment of a

train. Preliminary studies revealed that a derailment followed by a collision with a train from the opposite direction had a substantial contribution to the societal risk. Therefore, in the preliminary design and the requirements a derailment provision was included to prevent a derailing train to get into the free space profile of a train in opposite direction. The derailment of the ICE at Eschede triggered public concern, opening up a window of opportunity to implement such costly derailment devices. These derailment provisions had to be very strong structures to withstand the forces that resulted from a derailed train. The weak substrate in the Netherlands made it necessary to build large sections of the track on a concrete foundation. In the preliminary design the derailment provision was therefore integrated with this concrete construction. This resulted in a preliminary design for the concrete structure with small concrete walls that gave stiffness to the slab while functioning also as a derailment provision. This proved to be overall the cheapest way to ensure the derailment provisions. Simultaneously, rescue and emergency facilities could be accommodated in such a structure, enabling passengers to a self-reliant escape from a train in distress, provide access for rescue and emergency services and integrated their water supply in the structure. This multifunctional track concept became the reference design for the constructors in the contracting of the tracks.

The first parts to be built were the civil structures. Those parts were commissioned as a design and construct contract. The constructors were not responsible for the derailment safety of the trains. This was a shared responsibility of the infrastructure provider and the company that exploited the trains. The civil constructors adapted the design for the civil structures, simplifying the design for economy reasons. They found another way to ensure the stiffness of the construction. The concrete walls that had also a function in the preliminary design as derailment provision were left out. The infrastructure provider, who was responsible for the derailment safety, started their design almost two years later. He did not have the option to integrate the derailment provisions in the concrete structures anymore. His only option left was a construction between the tracks. This construction was much more expensive, and had the disadvantage that debris could become stuck between the derailment provision and the track, thereby posing a new hazard to the train operation. Moreover the derailment provision was the cause for additional maintenance and performance problems. Consequently, separate facilities for noise abatement by concrete fences were introduced, disabling access for rescue and emergency services. Instead, to provide sufficient surplus of water for these services, separate ditches and drains were added to the track bed, becoming an additional hindrance and cost inducing addition to the design.

The infrastructure provider, following the incentives in his design, build, finance and maintenance contract, tried to optimize the design in order to have the least maintenance costs and the best operational performance. They obviously had a strong case for leaving out the derailment provisions on a large part of the track. Incorporating the derailment provisions on straight parts of the track, would possibly even diminish the safety of the train, because the hazard of debris stuck in the derailment provisions, causing a derailment, outweighed the advantage of mitigating the consequences of a possible derailment. Their contract contained the reasonable clause that the derailment provision could be left out on places where the provision would be counterproductive.

Although the safety calculations made in the beginning of the project showed that it was overall cost effective to enhance safety by making derailment provisions, the overall result was a railway where the derailment provisions were left out over a large part of the track. While every designing actor in the process was optimizing his design on costs and safety, the result was, that a cost effective safety measure was left out, because it was not in the interest of any individual design actor in the process. The mechanism in this case shows that measures, contributing to safety of the total system tend to be postponed to parties acting later on in the process. While the cheapest way to contribute to safety is often at the start of the project, the sub-optimizations as shown in this case, make it difficult to implement them in the early stages of the project.

All major components of the HSL rail systems have encountered minor and major disruptions in their design and development process. Responses to these disruptions have varied widely from gradual optimization of existing solutions to conceptual change and innovative solutions. Derailment was triggered by the Eschede disaster, due to a technical design problem with the steel wheel rim. The problem of derailment by wheel rim failure was solved by redesign of the wheels. This redesign provided an adequate solution, making costly infrastructural provisions for containment of the rolling stock superfluous. Despite the realistic hazard of snow, this hazard was not addressed or investigated, despite experiences in the Alpine regions with snow accumulation. Derailment of trains in Japan and China due to cross wind and theoretical knowledge on dynamic wind loads on trains did not raise interest in this phenomenon, despite high bridges in the Western Scheldt estuary open landscape. Safety of tunnels became a major

issue after several serious fire events and lead to an innovative solution for the Green Heart tunnel.
In general, a multifunctional design as the consequence of an integrated concept requires design considerations at the functional level before the detailing of the design takes place. Such functional design considerations require oversight and understanding of the overall loads and limitations of the design. At the functional level, the design should be adaptive to unidentified and unanticipated hazards rather than accepting such hazards as negligible or acceptable due to their low probability.

3.3. The role of safety in assessment procedures

In due course, the HSL project triggered questions in Parliament about delays, cost overruns, track selection and the protection of the Green Heart as the environmental center in the Western part of the Netherlands. In 2004, this resulted in a Parliamentary Hearing on critical aspects of this major project. This Hearing included the safety aspects of the design and construct of the infrastructure and revealed four issues for concern. Throughout several previous infrastructural projects and successive evaluation studies, deficiencies were revealed in legislation, project process management, knowledge dissemination and independent safety assessment procedures. An equivalent procedure for assessing safety as a societal value, comparable to environments, economy and sustainability, proved to be absent [12].
While a generic framework lacked, object and project specific procedures became available for tunnels, shopping malls and parking lots. The scope of their assessment remained restricted to physical safety and the local level of public governance. This approach created project specific assessments, with considerable diversity, inconsistencies and variance across Safety Integrity Levels and Safety Case descriptions.
There has been an exclusive focus on Quantitative Risk Assessment techniques, applying specific external risk standards and norms for individual and group risk exposure. Only after several major events in the Netherlands like the firework explosion in Enschede a stringent focus on risk frequency and probability has been extended to consequences in terms of damage contours and population at risk. A standard assessment methodology for integral risk has been lacking, in particular with respect to subjective risk assessment and social acceptance of risk. In the public debate a shift has occurred from compliance with standards, to managing risk and assessing safety as a social value.
Finally, safety has been acknowledged as a strategic value on a societal level of decision-making. However, it lacks the methodology to develop risk into a practical approach in the detailed design phase on the operational level. Safety, independent of the materialized and specific form of its constructs, objects and artifacts cannot be traded off against other values, such as environment, economy or sustainability. Assessment at a tactical level of decision-making and on the level of functional requirements has not yet been achievable. Such a deficiency creates a repetition of decision-making steps, discussion on feasibility and acceptability of risk with –eventually- a suboptimal result [12]. Such risk decision-making procedures have been criticized for their assumptions and limitations due to the erosion it created in achieving consensus among stakeholders. An increasing judicial emphasis in decision-making emerged from the debates, due to the interrelation of liability and design deficiencies. Eventually, disputes were brought before the Supreme Court in the Netherlands in settling judicial liability claims. On an international level, Corporate Man Slaughter and Homicide Act (2007) legislation has aggravated the situation by the staggering extend of claims in case of product deficiencies.
Design and development liabilities caused risk-avoiding behavior with contractors in public-private partnerships. Conservative designs and policy-making strategies were favored, based on detailed regulations, standards and state-of-the-art technologies. The uncertainty margins that were chosen caused considerable cost overruns. A polarization in decision-making processes occurred, because negotiations became based on perceptions, cost-benefit considerations and political agenda. Available expertise and experience remained confined within private organizations and local authorities or were neglected as such. An increase in local decision-making was noticed in delegating decisions to lower levels of governance and organizations. General decision making criteria became submitted to locally dominated aspects in the efficiency-thoroughness trade-offs, losing transparency and consistency.
In such decision-making processes, inequality among parties in their access to information, methods and assessment procedures created disputes on the validity and credibility of decision support tools. It caused suspicion among the public towards rational decision making as such. Eventually the gap in the design process between goal and form as well as the gap in decision-making processes between strategy and operational levels triggered interest for the functional level of design and for decision-making at the tactical level.

3.4. ERTMS, a software issue

During the design and development of the software of the new ERTMS railway signaling system, numerous technical choices of a safety critical nature had to be made. Each of these choices had to be verified by testing and certification through notified bodies, based on the TSI functionalities that became available during the design and development process of the HSL project. This complex process did not only involve many steps in the development, but was also organized along lines of public-private partnerships of governmental agencies, the HSL project organization and manufacturers. Parts of the project only existed on paper while software specifications for the TSI were developed simultaneously with the design of the infrastructure and overall HSL system configuration. Contracted responsibilities and liabilities interfered with the development process, while an integral testing of the system performance was postponed and only possible once concrete products and software versions became available. Delays and cost overruns caused concerns in parliament, questioning the reasons and fairness of the delays, frequent upgrades of software versions, migration times and duration of testing periods [11].

During the investigations, the incremental progress of the design proved inevitable. Several decisions had successively passed their point of no return. In hindsight however, decisions could have been made differently:

- Off the shelf solutions were not available due to the choice for an innovative approach. Design of software ran concurrent with the development of functional requirements of the TSI's and specifications of the software.
- While the Netherlands applied an innovative approach for the Rotterdam-Antwerp corridor, Belgium applied a more incremental approach on their part of the system and track design. The systems transition between the two manufacturers of systems was chosen on the national border, instead of the system border, either in Rotterdam or Antwerp.
- The project insisted on a contract-based development of the 2.2.2 software version as an intermediate version, while 2.3.0 would be implemented as the new standard in reality. In the 2.2.2 software version, a consolidated version had to be defined to integrate the concepts of the HSL/governmental version and the industrial version which initially had been developed independently
- System integration was only foreseen, planned and to be tested in the final stages of the project, covering the interrelations between tracks, signaling, rolling stock, logistics, driver training and traffic control. Hot upgrades of the software would be implemented in practice during operations.
- The involvement of various major manufacturers of software, hardware and communication equipment created a complex technological challenge in establishing a consolidated 2.3.0 software version, harmonization of operational speeds across the network, interoperability at national borders and development and transition from a level 2 to a level 3 deployment of ERTMS. Development and integration to higher system levels transferred costs and risk from the infra provider to operators, while a series of hot upgrades in the near future remains foreseeable.

In addition to these technical issues, the certification of the software was dealing with unprecedented governance complexities. To cope with this complexity, recommendations were made regarding:

- Introduction of a Safety Case by the railway inspectorate, providing feedback of principles and standards to contractors
- Installation of a Task Force on the EU level to harmonize safety assessment procedures, comparable with aviation practices
- Reducing the variety of intermediate solutions, versions and products that emerged from the iterative and corrective developments, consolidating the existing complexity due to the inevitability of the ongoing process
- Registration and analysis of predicted and emerging operational mishaps on an EU level, sharing experiences in order to provide a timely transparency of systemic deficiencies.

3.5. The Fyra high speed train

In 2005, the first delays manifested themselves in a timely delivery of the rolling stock for the HSL [13]. The main issue was the delay of the ETCS equipment due to software issues, forcing the HSL trains to use conventional tracks and speeds instead of the newly constructed HSL tracks and high-speed connections. Testing and certification is done separately for the Belgian and Dutch train sets between 2009-2012, and become –although provisionally approved- operational in December 2012.

In January 2013 the Dutch operator –High Speed Alliance- issues a declaration that performance of the Fyra is satisfactory, despite the continued ETCS software deficiencies and disruptions. However, due to snowfall in January, the Fyra suffers damage and is withdrawn from operations. Shortly after one

another, the Belgian and Dutch government cancel the contract for further deliveries and return the rolling stock to the manufacturer Ansaldo Breda in Italy. These decisions are unprecedented. Similar manufacturing deficiencies with far more safety critical events, such as the wheel rim fracture of the ICE in the Eschede train disaster and the Lithium-Ion battery fires in the Boeing 787, have not had such drastic recalls and scrapping of the products. These decisions are made without consulting the NoBo's, following national approval procedures and without disclosure of the investigation reports to the manufacturer. Simultaneous problems with ETCS created a window of opportunity to raise public concern on the safety of rolling stock. Safety issues are used as an argument of opportunity to protect the interests of national railway manufacturers and operators [13].

3.6. External interferences

In practice, several external interferences have occurred with a completely different impact. The Eschede train disaster of 1998 has cost 101 lives and 88 injuries, creating concerns on high-speed derailment. Several preventive measures were proposed and designed for the Dutch HSL and successfully deleted in later phases of the project. Several tunnel fires lead to an EU wide Directive for tunnel safety, mandatory introduced in all new railway tunnel designs, irrespective the sometimes excessive costs. This Directive provided a window of opportunity for an innovative design of the Green Heart tunnel, integrating the functionalities of rescue and emergency in the conceptual phase of the design in an unprecedented manner, surpassing the reference design model. Continued safety problems in software design of ETCS delayed the delivery for many years, but did not lead to a revision of the perspective to implement a level 3 in ERTMS in the near future. In 1994 snowfall was assessed as a risk in an early phase of the project, and could have been tested and simulated based on existing climate wind tunnel facilities in Europe, but was considered negligible for the Dutch network operating conditions and was not further investigated. This snow item contributed in a drastic cancellation of rolling stock in 2013, after one month of operations.
Although heavy cross winds on high bridges were recognized in 1994 as a potential risk, they were dismissed as only train noise propagating intermediates and not further investigated. Crosswinds were not identified as a potential derailment cause despite accidents at Uetsu (Japan) in 2005, because -in contrast to aviation- there are no design limitations for gusts on dynamic train behavior.

4. Multi-actors

Modern infrastructural systems depend on many actors during design and operation. All these actors adapt in different ways. They all have different viewpoint about which variations are profitable and they all have a different decision mechanism about the variation that are allowed to become the basis of the best practice. Selection mechanisms are economic incentives, workload and risk aversion [1], [7]-[8], [10]. This may result in problems during the lifetime of the system. If parts of the system adapt in different ways, the system may become brittle, which can lead to malfunctioning or even accidents [16]. This is described as the phenomenon of 'drift into failure' [2], [14]. Such a concept of 'drift into failure' however is not restricted to the operational phase but can also be applied to decision-making during design and development. Corrective consultation of stakeholders and experts took place by organizing ad-hoc working groups and issuing independent investigations.
Altogether, the various decision making processes on the design, development and assessment have led to two Parliamentary Hearings. The first was organized in 2004, while the second is to be finished before the summer of 2015.

4.1. Intermediate conclusions: The HSL case

In the design of the infrastructural components of the HSL project, the judicial framework dominated over the technical design. In the ERTMS and rolling stock design, contractual obligations prevented a swift and effective transition in software upgrading and conversion to final versions that were implemented. The use of reference designs in software development did not work. The restriction to the functional design level left a variety of versions open for the final design that hampered communication of the different software versions across manufacturers. In the physical design domain, the Green Heart single tube tunnel completely replaced the double tube concept of the reference design. In later phases of the design, the initial reference track concept for the integral solution for track stability, underground foundation and accessibility for rescue and emergency services and ability of passengers to cope for themselves in crisis situations was decomposed in stand-alone components and single functions. This decomposition was made based on cost considerations and fallback to proven technology. Several unforeseen external events had a major influence on integrating safety into the design with

respect to acceptable risks of derailment, fire in tunnels, and terrorist threats. Several mitigating measures were taken after the events and later withdrawn or considered irrelevant or negligible at all such as snow and crosswinds.
Several studies concluded that there should be a group of independent technical experts -in fact a NoBo- to assess the capability of the manufacturers to modify their design to such an extent, that compliance was achieved with the requirements of the commissioners. Other events should not interfere with these assessments and certification processes, such as in the case of the Fyra and ETCS deficiencies.

4.2. Towards resilience in major projects

In reflecting on the results of the HSL project, each of the system components has seen considerable adaptation. Some components were only recognized as safety critical late in the process, while functions were re-assessed with respect to their criticality based on external influences, such as derailment, terrorist threats or snow and wind. To this purpose, several ad-hoc working groups were installed. Although a wide divergence in the decision-making was recognized, no precautionary measures or fallback options were applied. Lead-time and cost considerations prevailed in a dominantly judicial framework. Due to the unique and innovative nature, off-the-shelf solutions were not available, while reference designs were abandoned for opportunistic reasons. Risk assessment tools and techniques changed during the process, shifting from strictly rational to perceptional aspects and achieving consensus.
The DCP diagram (figure 2) shows the positioning of resilience in the functional phase in design. This diagram indicates the various steps in design, control and practice in complex systems. In answering the rhetorical question of this paper: yes, we can cast resilience in concrete, but only when the intermediate steps between system goals and physical forms are clearly defined and an encompassing oversight over the functionalities is achieved and tactical decision making is coordinated and transparent.
After a conceptual level and strategic decision-making phase, the design and development rapidly moved to the detailed design and local implementation level of governance. This rapid shift to detailed design was rationalized by the public-private partnership concept. This concept leaves a high degree of autonomy to manufacturers, construction companies and local decision making arenas under the motto: Process drives out content, the knowledge is in the market. At these detailed levels, a wide variety of requisite solutions emerged, leaving little room for oversight and control over trade-offs with costly consequences and modification delays.

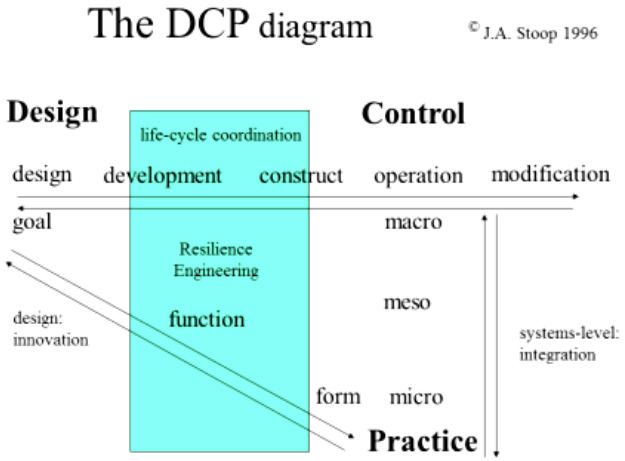

Figure 2. Resilience in the functional phase of system development

During this process, the functional level and tactical decision making level was only marginally addressed. At this level however, a functional oversight, flexibility and consistency of design solutions could have been realized before they were cast in concrete. It remains an open question to what extent resilience engineering at this functional level could have had a positive contribution to the eventual result.
Three systems levels can be distinguished; on the lowest level the dynamical properties of the system that is being designed; on the intermediate level the adaptation properties of the system and on the highest level the control of the adaptation processes. Decisions on the control level determine how the system adapts; adaptation changes the dynamical properties of the system. During the design stage, the system adapts very quickly. In the HSL case the design was allowed to adapt freely, resulting in suboptimal solutions. At this functional level a specific role for an architect becomes visible. On one hand there is a need to maintain oversight and comprehension over the technological properties of the system as such, based on domain specific knowledge and design experience. On the other hand, the interrelations between hardware, software and life ware aspects require interface management and transition strategies across the various project phases in an understanding of process and governance control mechanisms. Technical knowledge is a prerequisite to effective control of the adaptation process in the design stage.

5. Conclusions

Based on the observations of the dynamics of the decision-making processes in the design and development of the High Speed Line railway project, the following conclusions can be drawn:

- The commissioner should focus on the question whether the incentives drive the actors to a consistent and resilient system.
- This asks for a strategic engineer or architect, whose task it is to understand how incentives and requirements influence each other and to safeguard the future possibilities of the system.
- This strategic engineer should be involved in the project from the moment requirements and incentives are formulated.
- In resilience assessment the mechanisms that exist in the system, should be studied, in order to determine what the potential of adaptation of the system is.
- A discrimination between different levels of change should be taken into account: optimization of existing solutions, adaptation of the design to additional functional requirements, and innovation in order to eliminate issues that cannot be overcome by intervention in the existing design and configurations.
- The interrelations with other design aspects with their intended and predicted performance should be assessed beforehand in order to prevent 'emergent' properties and unforeseen side effects during operations.

References

[1] Cook, R.I. & Rasmussen, J. (2005). Going Solid: A Model of System Dynamics and Consequences for Patient Safety. *Quality & Safety in Health Care*, *14*(2), 130-134.

[2] Dekker, S. (2011). *Drift into failure*. Ashgate, Aldershot, England.

[3] ESReDA (2015). *Case study analysis on dynamic learning from accidents. The ESReDA Cube, a method and metaphor for a learning space.* Project Group on Dynamic Leaning from Accident Investigation. European Safety and Reliability Data Association, March 2015.

[4] Evers. J, Bovy, P., De Kroes, J.L., Sommenhalder, R., & Thissen, W. (1994). Onderzoeksschool TRAIL, Transport, infrastructuur en logistiek: Een proeve van een integrerend onderzoekprogramma. Publicatie 94/1. (in Dutch)

[5] Holland, J. H. (1992). Complex adaptive systems. *Daedalus*, *121*(1), 17-30.

[6] HSL (1994). Nieuwe HSL-Nota. *Deelrapport 18 Spoorbaanconcepten. Deelrapport 19. De grote kunstwerken.* Projectbureau HSL-Infra. (In Dutch)

[7] Kahnemann, D. (2012). *Thinking Fast and Slow.* Penguin, London, England.

[8] Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, *27*(2/3), 183-213.

[9] Slobodkin, L.B. (1964). The strategy of evolution. *American Scientist*, *52*, 342-357.

[10] Slovic, P. (1999). Trust, emotion, sex, politics and science: Surveying the risk-assessment battlefield. *Risk Analysis*, *19*(4), 689-701.

[11] Stoop J.A., Baggen J.H., Vleugel J.M., De Kroes J.L., & Vrancken J.L.M. (2007). HSL-beveiligingssysteem ERTMS. Een onafhankelijk onderzoek naar nut en noodzaak van de aanpassing van het HSL-beveiligingssysteem ERTMS. Onderzoek in opdracht van Onderzoeks- en verificatiebureau Tweede Kamer der Staten generaal. Technische Universiteit Delft, May 2007. (In Dutch)

[12] TCI (2004). *Hoofdstuk 10. Veiligheidsborging van grote infrastructuurprojecten*. In: Onderzoek naar infrastructuurprojecten. Tijdelijke Commissie voor de Infrastructuur. Tweede Kamer der Staten Generaal, Vergaderjaar 2004-2005, kamerstuk 29283, December 2004. (In Dutch)

[13] Walta W. (2013). *De Fyra: een Europees drama.* Stichting Maatschappij en Veiligheid, SMV. (In Dutch)

[14] Woods, D.D. (2003). Creating Foresight: How Resilience Engineering can Transform NASA's Approach to Risky Decision Making. (Testimony on The Future of NASA for Committee on Commerce Science and Transportation, John McCain, Chair).

[15] Woods, D.D. (2014). *Velocity NY 2014 Keynote: The mystery of sustained adaptability*. http://www.youtube.com

[16] Woods, D.D., Schenk, J. & Allen, T.T. (2009). An Initial Comparison of Selected Models of System Resilience. In C. P. Nemeth, E. Hollnagel, & S. Dekker (Eds.), *Preparation and restoration* (Vol. 2, pp. 73-94). Ashgate, Aldershot, England.