The Safe System Approach – A Road Safety Strategy Based on Human Factors Principles

Peter Larsson[1,*] and Claes Tingvall[2]

[1] Swedish Transport Agency, Borlänge, Sweden
[2] Swedish Transport Administration, Borlänge, Sweden
peter.larsson@transportstyrelsen.se,
claes.tingvall@trafikverket.se

Abstract. In most safety critical domains, safety has been improved through the application of contemporary human error models and management methods. But the common strategic approach to improve road safety has so far mainly been built on the view that individual road-users utterly are responsible when crashes occur and countermeasures have consequently been aimed at changing the behaviour of the road-user. This approach is however slowly shifting and there is a growing understanding that the strategies must be based on human factors principles. In this paper the human factors principles of the Safe System approach are outlined and important implications for the design and regulation of the road transport system will be presented. It is concluded that the Safe System approach share vital foundations with the human factors concept. But it is argued that the Safe System approach takes the human factors approach further by regarding the capability of the human body to withstand external influences with a potential to induce bodily harm.

Keywords: Human Factors, road safety, Vision Zero, system safety, road users, Safe System approach, safety.

1 Introduction

The development of road safety is undergoing major changes now and most certainly in the next ten years. The global community has reacted strongly on the predictions of the impact of poor safety and the growth of road traffic, on the society and the health of the population. It has been estimated that death through a traffic accident will become the third or fourth most common source of death within 10-20 years, unless major and effective actions are taken. The UN has declared 2011-2020 as "the Decade of Action" asking for contributions from all countries and stakeholders to diminish a world epidemic of road casualties that has not only an impact on health but also on economy and economic growth in particular in low and middle income countries. The concern is related to safety, but the overall aim of the future is to develop a sustainable transport system where safety, environment, energy and accessibility are integrated. Such integration is complex and system design necessary as a tool to find synergies and limitations.

D. Harris (Ed.): EPCE/HCII 2013, Part II, LNAI 8020, pp. 19–28, 2013.

To meet this epidemic there is a growing understanding that the strategic approach to road safety must evolve. In most safety critical domains, safety has been improved through the application of contemporary human error models and management methods (Sheridan, 2008). However it seems that this approach to a rather high degree has been neglected by the road safety community (Stanton and Salmon, 2009). The common approach to improve road safety has so far mainly been built on the view that individual road-users utterly are responsible when crashes occur. As a consequence countermeasures have been aimed at changing the behaviour of the road-user in order to adapt him/her to the road transport system and making their behaviour free from human errors (e.g. Salmon et al., 2010; Larsson et al., 2010). Since the road transport system can be seen as a complex socio-technical system (e.g. Salmon et al., 2012; Larsson et al., 2010), such an approach has its limitations in extensively reducing the number of fatalities and severe injuries.

There has been a shift in the strategic approach to road safety for the last ten years. The pace of this process has been slow but there is now a growing understanding in the road safety community that the strategies must be based on human factors principles and system theories.

Current approach to road safety in large parts of the world is “Vision Zero” or “Safe System”, two expressions of an identical policy. Recently, in the white paper on transport “Roadmap to a single European transport area —Towards a competitive and resource efficient transport system “ the European Commission has adopted Vision Zero, with the target that by 2050, the number of fatalities due to road traffic crashes should be close to zero. Also the guiding principles underlying the global Plan for the Decade of Action are those included in the Safe System approach. The forthcoming ISO 39001 management standard for traffic safety specifies that the standard is only relevant for organizations that wish to eliminate death or serious injury in road traffic crashes. OECD/ITF (2008) has recommended that the Safe System approach should be used to manage road safety. In the private sector, Volvo Cars has set a target of zero deaths and serious injury in or by a Volvo car 2020. Other car manufacturers have expressed zero as their vision, but not specified when this is supposed to be fulfilled. All these examples have one thing in common, except from explicitly aiming for elimination of death as a result of road traffic crashes, and that is the human factors perspective.

2 Human Factors

Going through the literature it is hard to find a clear, simple and commonly agreed definition of the human factors concept.

According to the Swedish Human Factors Network (HFN) human factors is:

“the scientific discipline that investigates and produces knowledge concerning human physical, cognitive and psychological prerequisites in relation to the character of the task, technical requirements with respect to design, complexity, and organizational premises regarding resource allocation, organizational culture, methods, competence and leadership as well as following up and evaluating systems.

The utilization of the knowledge about human capabilities and needs in design, implementation, deployment, operation and maintenance of products, systems (of humans, machines and organizations) in order to optimize system functionality as well as human wellbeing, health and safety."

From this definition and other similar definitions it can easily be understood that human factors is a wide and rather complex scientific discipline embracing different subjects from ergonomic issues, e.g. Human Machine Interface (HMI), to safety culture and resilience in large organizations. It is however clear that the discipline has a common aim of managing human error by setting out from the physical, cognitive and psychological prerequisites and limitations of the human being in her interaction with other components of a complex socio-technical system in a social, organizational and often rule based context. The aim is hence to create optimal system conditions for the human being to be able to act as safely as possible in such a system by eradicating or reducing human error.

From the different definitions it is hard to derive some distinguishing and operationalized features to which the Safe System approach easily can be compared. But the following two central "axiom" or principles, can be derived from the definition.

2.1 Human Capability

The individual or person approach to safety management is still common in complex socio-technical systems e.g. occupational safety (Leveson, 2011). Leveson (2011) states that this approach is built on the assumption that most accidents are caused by operator error and rewarding ‘‘correct" behavior and punishing ‘‘incorrect" behavior will eliminate or reduce accidents significantly. According to Read et al. (in press) the individual approach views the person as another component of the system and recommendations are made for increasing the reliability of this component. Read et al. (in press) further states that little consideration is given to the context of behavior and its influence. Consequently the individual approach leads to proposals for countermeasures aimed at behavior change through education and enforcement that increase compliance with laws, internal regulations, routines etc.

The human factors discipline instead acknowledge the human frailty and clearly shows that human beings cannot physically, cognitively or psychologically always cope with the complex demands of socio-technical systems (e.g. Dekker, 2002). For that reason there is a need to understand the human capabilities in relation to the system and how to adapt the properties of the system to these capabilities.

2.2 Systems Approach

Acknowledging human frailty the human factors discipline treats human error as a systems failure, rather than solely an individual operator´s failure (Salmon et al., 2010). It considers the interactions between humans and between humans and technology within a system and the presence of system wide latent conditions and their role in shaping the context in which operators make errors. Human error is no longer seen as the primary cause of accidents. Instead it is considered as a consequence of latent failures created by decisions and actions within the broader organizational, social or political system in which processes or operations take place (e.g. government, local authorities, organizations/companies and their different management levels) (Salmon et al., 2010). At least in principle, the systems approach is now the dominant approach in most safety critical domains where it is often denoted Human Factors or MTO (Man, Technology and Organization).

Elaborating the concept of systems approach further, Leveson (2002) and Hollnagel (2004) mean that accidents can be seen as emergent phenomena. Accidents occur when components of a system interact with each other and these interactions are not possible to foreseen because of their complexity. According to Leveson (2002) systems theory provides the theoretical foundation for systems engineering, which views each system as an integrated whole even if it is composed of diverse individual and specialized components. A basic and important assumption of systems engineering is according to Leveson (2002) ‘‘that optimization of individual components or subsystems will not in general lead to a system optimum; in fact improvement of a particular sub-system may actually worsen the overall system performance because of complex, non-linear actions among the components”. This means e.g. that safety cannot be optimized through the optimization of the safety performance of the individual components and according to Leveson (2002) ‘‘attempts to improve long-term safety in complex systems by analyzing and changing individual components have often proven to be unsuccessful over the long-term”.

3 Basic Design Principles of the Safe System Approach

According to Langford (2009) Sweden’s *Vision Zero* and the Netherlands’ *Sustainable Safety* represent the longest established Safe System approaches. Langford (2009) describes that such approaches around the world have the following common key features:

- “they recognize that the human body has a limited tolerance of violent forces and when crash energies exceed this tolerance, death or serious injury will be a probable outcome;
- they accept that crashes will continue to occur, accident prevention efforts notwithstanding, given that humans make mistakes when using the road system;
- the challenge for any Safe System in the event of a crash is to ensure that no fatalities will occur (and that serious injuries will be reduced) for road users behaving appropriately; and
- this challenge can be best met by managing the road infrastructure, vehicles and speeds to reduce crash energies to levels that can be tolerated by the human body.”

Langford (2009) means that Safe System approaches clearly differ from traditional views of road users. One example is the Netherlands’ *Sustainable Safety* which considers the road user the weakest link in the transport chain. According to Langford (2009) the individual road user “is largely unpredictable and cannot be relied upon to behave safely over the long term, all of his or her best intentions notwithstanding. People make mistakes. Training, education and even enforcement measures which rely upon correcting road user behavior will not succeed in achieving Safe Systems' ambitious goals."

The basic principles of the Safe System approach is further elaborated and summarized by the following design principles.

- *The design of the road transport system should guide the road user to a safe behaviour and mitigate the consequences of common human errors.*

The overarching concept of a safe transport system contains two imperatives, known for thousands of years. The first is that "it is human to err" (errare humanum est) meaning in this particular case that the human can never be trusted to repeatedly perform correct in all traffic situations, even if the intention is to maneuver in a safe manner. Hence the capabilities and limitations of the human being must to a great extent be taken into consideration when designing the road transport system. Road users will always make errors and mistakes for various reasons. These errors and mistakes in many cases originate from the interaction between the road user and the complex social, organisational and technical context in which the behaviour of the road users take place. They hence may be reduced by understanding these interactions and designing the road transport system from these conditions in order to guide the road user to an as safe as possible behaviour.

The other imperative, today well and thoroughly verified, is the role of kinetic energy in case of a human error. Hippocrates wrote around 400 B.C (Adams (ed.), 1886):

"Of those who are wounded in the parts about the bone, or in the bone itself, by a fall, he who falls from a very high place upon a very hard and blunt object is in most danger of sustaining a fracture and contusion of the bone, and of having it depressed from its natural position; whereas he that falls upon more level ground, and upon a softer object, is likely to suffer less injury in the bone, or it may not be injured at all."

What is behind Hippocrates sentences is simply the strong relationship between the speed/energy and the object that finally stops us in case of a human error leading to a crash, and how such errors can be counteracted with lower speed and/or substituting or modifying surfaces that we hit. A high risk of human error can therefore be matched by reduced kinetic energy or less harmful contact surfaces.

Since human errors and mistakes cannot fully be eradicated, the infrastructure components and vehicles of the road transport system must be designed to mitigate the consequences of common human errors and mistakes. While this may be clear and logic, the road transport system has not been designed from ground with the aim to absorb or mitigate common human error or to absorb the consequences of it.

The Safe System approach combines the two imperatives with back casting. If zero deaths and serious injuries are to be achieved, how do we combine human error with human biomechanical tolerances by minimizing human error, but when it occur to make sure that the human biomechanical tolerance is not exceeded? In doing so, it is simply necessary to develop design principles for system safety, and not simply treat each component individually. The characteristics of the road user, the vehicles, the road design and the speeds on a road all have to work together to achieve safety.

- *The setting of speed limits must be in accordance to the safety standard of the infrastructure and the type of vehicle in such way that normal and common human errors and mistakes can be managed as to eliminate the risk of serious injuries.*

The preconditions for designing a safe road transport system are twofold; the biomechanical tolerance to mechanical force and the possible crash scenarios that can be foreseen. In working out possible scenarios, the human behavior is the key for understanding what might lead to a crash with energy enough to harm the human. A high risk of human error can be matched by reduced kinetic energy or less harmful contact surfaces. The balancing act is to maintain accessibility and mobility of the road transport system, but limitations in safety should be counteracted by reduced kinetic energy, which in most cases mean reduce speed. The alternative to reduce speed is an investment into the system that leads to maintained or even increased speed. This is why progressing in safety in the end is an investment in mobility.

- *New rules and regulations with the purpose to change human behavior must be developed from a human factors perspective taking into account the limitations and capabilities of the human being.*

There is still a fairly widespread belief that accidents are caused by human errors and that these could be significantly reduced by introducing additional regulations and procedures to ensure a "correct" behaviour and punish an "improper" behaviour of those who "violate" the rules. This approach presupposes that human errors are more or less intentional violations, i.e. that the road user in all situations can make a deliberate or conscious decision to act right or wrong. Running a red light or trying to cross an intersection despite there is conflicting traffic are typical examples of serious traffic offences that might have no intention behind. Forgetting to put on the seat belt, not turning on headlamps, losing control on a road with invisible ice are other such examples of violating the traffic rules with no real intention behind, but possibly leading to lethal consequences.

On a general level human error in road traffic hence can be divided into unintentional errors (mistakes, slips, lapses etc.) and intentional violations. Contemporary Human Factors research clearly shows that regulating human behaviour and making the individual accountable for accidents will only have marginal effect on unintentional errors (e.g. Dekker, 2002). In depth analyses of road traffic accidents show that such errors are common contributing factors.

When it comes to intentional violations Svensson (2008) shows that such regulating activities will have an effect but it varies considerably with the risk of being caught and the level of sanctions.

Speeding, driving under influence of alcohol or other drugs, not using restraint systems or not using protective equipment are in many cases serious intentional violations but in some cases unintentional errors (especially when it comes to speeding, not using restraint systems and protective equipment). These violations and errors may lower the effects of the system design and must be met with special attention.

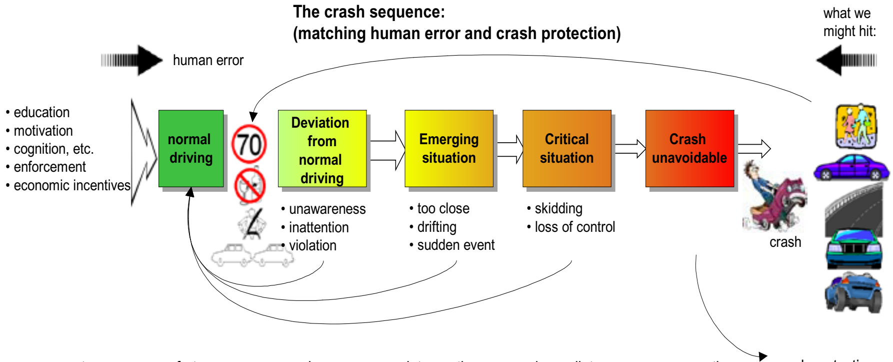
- *Design solutions of the road transport system and rules and regulations with the purpose to change human behavior must be evidence based and based on an integrated systems approach.*

The development of road safety should and must be based on scientific evidence and best evidence from experience. This should apply to all stages of the development, from target setting and management to detailed design solutions and regulating efforts to diminish or eradicate trauma. In doing so, it is necessary to integrate safety solutions to all factors of an accident and injury prevention process. This is a general trend in the automotive sector since a few years back, but needs to be broadened to the entire road transport system. To seriously reduce e.g. pedestrian casualties, road user rules and behaviour, road and traffic environment, speed management, systems to brake a car automatically and "pedestrian friendly" front ends cars must be combined in an optimised way. In isolation, the effect of each component may have some effect, but as they give each other preconditions to maximise benefit, the whole combination might give more effect than the sum of each component.

The possibility to build a safe road traffic system on an overall level is not complicated. The aim of such a system is to make sure that the biomechanical tolerance for a fatal or serious injury is not exceeded. Setting out from the so called integrated safety chain in fig. 1 the system should be designed backwards from a possible event where injury might occur. The challenge is to prevent the hazardous event at as early as possible stages of the integrated safety chain but simultaneously acknowledge that this is not always possible and hence take measures to limit the amount of energy that might be exchanged in case of a crash. At a later stage in the chain, safety systems that can limit the risk of an injury given a crash can be activated. The key is to link the possible outcome with the speed that can be tolerated under normal driving conditions so that the amount of kinetic energy is not larger than what can be managed through the chain. The real challenge is both to combine the links of the chain to what is most effective, and to evaluate the combined effects.

For each step in the chain, a systems approach must be taken in order to understand and integrate road user rules and behaviour, road and traffic environment, speed management, vehicle systems with the aim to combine them in an optimised way.

Even if harmful events cannot be prevented and returned to an earlier stage of the chain they can be transformed in order to make it easier to mitigate their consequences in following stages by e.g. a more favourable crash configuration. One example is Electronic Stability Systems (ESC). Even if a vehicle comes over into the oncoming traffic lane, the risk of doing it with the side hitting oncoming traffic resulting in an unfavourable crash configuration is minimized. It is important to understand that efforts should be put in all parts of the chain but it is not possible to always rely on solving the problems in earlier stages of the chain. There will always be events that "falls through" the chain and the only way is then to mitigate the consequences.



• access to road transport system	• comfort • economy • social conformity	• warning system • supporting system	• intervention in driving	• immediate correction	• preparation for crash	crash protection
Vehicle	promote normal driving	(ISA, SBR, alcohol interlock)	(AICC, LDW)	(ESC, LDA, AICC2)	(pre-safe, emergency braking)	(seat belts, airbag, whiplash protection, pedestrian protection)
Infrastructure	promote normal driving	(speed warning, tactile warning, humps)	tactile edge lines	high friction surface		barrier design, roundabouts
Others	promote normal driving	• enforcement • insurance • contracts				• emergency service

Fig. 1. The integrated safety chain (Tingvall et al., 2009)

4 Discussion

From the design principles it seems clear that the Safe System approach share many features of the view of human capability and the systems approach with the human factors concept.

The maybe most obvious common feature of the two concepts is that they both acknowledge that human beings cannot physically, cognitively or psychologically always cope with the complex demands of socio-technical systems, like the road transport system. Instead the human factors discipline and the Safe System approach urge us to understand that when the human is a part of a complex system he/she cannot always act safely or perfectly according to the rules even if his/her intentions are correct. Such systems must consequently be designed and operated with the capabilities and limitations of human beings as a starting point.

Another important common feature, which is closely related to the previous feature, is that accidents can be seen as emergent phenomena (Leveson, 2002 and Hollnagel, (2004) and that optimization of individual components for that reason will not in general lead to a system optimum. This is an important conclusion since it states that safety cannot be optimized by e.g. trying to optimize the safety performance and behavior of the human being or any other component of a complex system. The Safe System approach consequently emphasizes the importance of understanding and integrating road user rules and behaviour, road and traffic environment, speed management, vehicle systems with the aim to combine them in an optimised way.

However it can be argued that the Safe System approach takes the concept further creating a more holistic systems approach to road traffic accidents.

According to Read et al. (in press) the field of human factors has traditionally focused on the physical and cognitive capabilities and limitations of humans aiming at the understanding of human error and how it can be managed or controlled. Read et al. (in press) however claims that modern human factors approaches are moving away from the psychological approach that considers humans as limited information processors. Still human capabilities and limitations are important to understand but a greater focus must be put on the context of behavior and the constraints imposed by the environment.

From these statements and the previous mentioned definition by HFN it can be argued that the human factors discipline seems to be mainly focusing on managing and controlling human error in order to avoid accidents. It seems that the main focus of human factors is the understanding of behavioral aspects in relation to the system context.

The Safe System approach also embraces the management and control of human error. However it also focuses on mitigating the consequences of such errors. This dual view on human error is illustrated by the integrated safety chain (fig. 1).

The integrated safety chain share many common features with nuclear safety and the principle of "defense in depth". According to IAEA (1996):

> "Defense in depth is generally structured in five levels. Should one level fail, the subsequent level comes into play. The objective of the first level of protection is the prevention of abnormal operation and system failures. If the first level fails, abnormal operation is controlled or failures are detected by the second level of protection. Should the second level fail, the third level ensures that safety functions are further performed by activating specific safety systems and other safety features. Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials. The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response."

But there seems also to be an important difference between the integrated safety chain and "defense in depth". The outcome of each step of the integrated safety chain, once it did not stop the event, is an input to the next step. Therefore, each step must have to design properties, either to stop the chain or prepare for the next phase. It should though be noted that the principle should be not to let many cases run to far in the chain of events and run the risk to be stopped by the last barrier.

From the literature it is quite unclear if the Human Factors discipline embraces these aspects of system perspective regarding the physical frailty of the human being and the way it can be mitigated even if e.g. Hollnagel (2004) is considering material or physical barrier systems important for the blocking or mitigation of an unexpected event. This may be due to the fact that in systems where the concept of human factors and system safety have evolved in safety critical systems where the levels of harmful energy have not been possible to mitigate in an effective and economic way.

However it seems that the last step in the integrated safety chain, preventing or mitigating the consequences of human error, is omitted or at least not clearly elucidated in the human factors approach. Thus the Safe System approach takes the view of human capability and systems approach a step further compared to the human factors approach by adding the biomechanical tolerance and its implications on systems design.

References

1. Adams, F. (ed.): The Genuine Works of Hippocrates. William Wood and Company, New York (1886)
2. Dekker, S.W.A.: The Field Guide to Human Error Investigations. Ashgate Publishing Limited, Hampshire (2002)
3. Hollnagel, E.: Barriers and Accident Prevention. Ashgate Publishing Limited, Hampshire (2004)
4. IAEA.: Defence in Depth in Nuclear Safety, INSAG-10. International Atomic Energy Agency, Austria (1996)
5. Langford, J.: Towards Zero: Understanding a Safe System Approach to Road Safety. Fact Sheet No. 1. Curtin-Monash Accident Research Centre, School of Public Health, Faculty of Health Sciences, Curtin University of Technology, Perth, Western Australia (2009)
6. Larsson, P., Dekker, S.W.A., Tingvall, C.: The need for a systems approach to road safety. Safety Science 48, 1167–1174 (2010)
7. Leveson, N.G.: System Safety Engineering: Back To The Future (2002), http://sunnyday.mit.edu/book2.pdf (retrieved October 18, 2006)
8. OECD/ITF.: Towards Zero: Ambitious Road Safety Targets and the Safe System approach. Summary document. OECD Publishing (2008)
9. Read, G.J.M., Salmon, P.M., Lenné, M.G.: Sounding the warning bells: The need for a systems approach to understanding behaviour at rail level crossings. Manuscript submitted for publication. Applied Ergonomics (in press)
10. Salmon, P.M., Lenné, M.G., Stanton, N.A., Jenkins, D.P., Walker, G.H.: Managing error on the open road: The contribution of human error models and methods. Safety Science 48, 1225–1235 (2010)
11. Svensson, M.: Sociala normer och regelefterlevnad – Trafiksäkerhetsfrågor ur ett rättssociologiskt perspektiv. Doctoral thesis, Lunds University, Lund, Sweden (2008)
12. Tingvall, C., Eckstein, L., Hammer, M.: Government and Industry Perspectives on Driver Distraction. In: Christie, K., Lee, D., Regan, M. (eds.) Driver Distraction. Theory, Effects and Mitigation. CRC Press (2009)