Reliable, resilient; towards a dialectic synthesis?

E. A. van Kleef
J.A. Stoop

Infrastructural and transportation systems have become more and more complex. They both have the characteristics of adaptive socio-technical systems. Understanding the true functional relations and couplings in such systems has become challenging. The situation awareness of designers and operators is compromised.

Reliability and safety tend to be assessed in a probabilistic way. Although probabilistic analyses can give great insight into a system's reliability and safety, it lacks understanding of dynamical failure modes.

In constructional safety several limit states are taken into account. The serviceability limit state is related to the criteria governing functionality, durability, user comfort and appearance. Ultimate limit states are related to situations that jeopardize people's safety or safety of the structure. In order to cope with systems dynamics, the notion of resilience has been developed. Reliability, safety and resilience can be considered concentrically notions. They are not conflicting but should be taken into account simultaneously. In dynamical systems a set of limit states or envelopes also exists, defining and allocating responsibilities between infrastructure, process control and human operator performance. Such allocation aim to facilitate recovery and return to safe and stable system states.

The possible states of the system can be described with a system state diagram. In such a diagram the set of states where the system is within its design limits and operator's focus can be on performance is bounded by the operating envelope. Outside the operating envelope, focus should be on safety and damage mitigation. The conditions where damage occurs form the viable envelope. After the occurrence of damage the focus changes to survival and resurrection, a focus that is known as resilience. If the limits of resilience are reached, the old system can no longer be reestablished and innovation is necessary.

This paper describes the relations between those envelopes in adaptive socio-technical systems and thereby offers a way to regain awareness of the system's dynamic behavior among designers and operators.