Systemic Resilience Model

Jonas Lundberg (Corresponding author)
Div. Media and Information Technology
Department of Science and Technology
Linköping University
SE-60174 Norrköping, Sweden
jonas.lundberg@liu.se
+46 11 363452

Björn JE Johansson
Div. Human-Centered Systems
Department of Computer and Information Science
Linköping University
SE-58183 Linköping, Sweden
bjorn.j.johansson@liu.se
+46 70 9277324

Abstract. It has been realized that resilience as a concept involves several contradictory definitions, both for instance resilience as agile adjustment and as robust resistance to situations. Our analysis of resilience concepts and models suggest that beyond simplistic definitions, it is possible to draw up a systemic resilience model (SyRes) that maintains these opposing characteristics without contradiction. We outline six functions in a systemic model, drawing primarily on resilience engineering, and disaster response: anticipation, monitoring, response, recovery, learning, and self-monitoring. The model consists of four areas: *Event-based constraints*, *Functional Dependencies*, *Adaptive Capacity* and *Strategy*. The paper describes dependencies between constraints, functions and strategies. We argue that models such as SyRes should be useful both for envisioning new resilience methods and metrics, as well as for engineering and evaluating resilient systems.

Keywords: Resilience, Systemic model, Self-monitoring, Safety II, Adaptive systems

Accepted on March 5, 2015, for publication in **Reliability Engineering & System Safety**, for the special issue on Resilience Engineering. DOI:10.1016/j.ress.2015.03.013. *This is a pre-print version (before copy-editing)*.

1 INTRODUCTION

The interest in adaptive systems lately can be seen as a reaction to the ever-increasing complexity and coupling (and intractability) of modern socio-technical systems [1]. While the 'old' technical systems surely could be seen as 'complex', they still were decomposable to an extent that made them understandable or at least possible to describe in detail, and thus assumed to be possible to control.

Today, almost all socio-technical systems are open 'systems-of-systems' [2], which are very difficult (if not impossible) to get an overview of, or even to define boundaries of, forcing us to surrender to the possibility that we never will be able to predict all possible states and associated outcomes that can emerge [1]. Traditional methods in safety engineering therefore struggle to keep up with the development of new technologies and usages of the same. The main drawback of such methods is that they are founded on an assumption of a certain degree of predictability and decomposability. These approaches have lately been labelled "Safety I" [3]. New concepts, such as 'resilience engineering' have gained attention. A common foundation for these concepts is that they all focus on adaptive capacity to stay in control when facing unforeseen disturbances or events, labelled "Safety II". Johansson & Lundberg [4] and Lundberg & Johansson [5] has similarly used Holling's [6] terms "stability" and "resilience" in a similar fashion when discussing the difference between safety strategies focusing on encapsulating or eliminating risks in contrast to adaptive strategies to cope with uncertainty and dynamics.

Resilience engineering recognizes that failure and success both originate from the same source, namely the inherent variability of performance in a socio-technical system. Patterson et al [7, p. 35] defined resilience as "Resilience is the broad application of failure-sensitive strategies that reduce the potential for and consequences from erroneous actions, surprising events, unanticipated variability, and complicating factors."

As [8] summarizes, from the perspective of disaster response, there are (at least) four resilience concepts in the literature. We observe that they are somewhat contradictory. Firstly, resilience can be seen as *robustness or resistance* on the one hand, versus *adaptive capacity* [6] on the other. The question then arises, does a resilient system resist adverse conditions, or does it adapt to them? (If it does both, what is the balance?) If resilience is about 'bouncing back' [9] (or 'bouncing forward' to a more desirable state) (e.g. [10]), how do we determine where it will go? Secondly, putting forth resilience as *recovery* [11] raises the question of whether a resilient system is resists adverse conditions, adapts to them, or simply is able to rise from the ashes, bouncing back from damage? Finally, resilience can be conceptualized as *preparing* [12], to adjust to what might be on the horizon, but also as ability to respond [13]. Is resilience then about a being proactive or is it about being reactive (during or after events)? Resilience can also encompass both (proactive adjustment and recovery) [14]. Similarly, [15] describe four resilience types, relating them to different resilience research traditions. Furthermore, while Manyena [11] emphasize that resilience should be an intrinsic ability, other authors have pointed out the contrary, that boundary spanning (the ability to reach out to others) is a resilience characteristic [16]. Indeed, there has been a concern that resili-

ence may have become a meaningless term, that "the term 'resilience' may collapse into the meaninglessness that results from having too many meanings." [17, p 198].

There is thus a challenge to present a resilience model that resolves these apparent contradictions without simply making resilience a synonym for something else, be it flexibility or robustness. To meet this challenge, we need to understand what the core functions of resilient systems are, and what the relations between them necessary to fulfill the demands are. Over the last ten years, the authors have developed these ideas [4, 5, 18-26]; which now are applied in the following model, called SyRes (Systemic Resilience Model). The model is systemic – focusing on constraints emerging from the system context, from functional dependencies, and from resilience strategies. Below, we describe how the SyRes model resolves the apparent contradictions between previous resilience definitions, providing a workable framework for envisioning and evaluating resilience metrics and models.

2. FRAMEWORKS FOR UNDERSTANDING AND STUDYING RESILIENCE

Theoretical models are implicitly or explicitly reflected in applied methods and metrics, e.g. as has been shown in accident investigation [27]. Therefore, a framework or a theoretical model can have major impact on later applied work, both by outlining what core aspects applied models should include, and through being used as a baseline for evaluating applied methods and methodologies. Below, we outline core functions of Resilience Engineering and Crisis response in different frameworks, highlighting how they overlap and diverge. This will then form the basis for a model focusing on relations and constraints between events and core functions.

To speak of resilience, something must stay constant while other aspects change. We suggest that the core identity, the "self", of a system should remain the same. By "system", we refer to an open socio-technical system working towards one or more meaningful, safety critical, goal(s) in an environment that holds the potential of presenting threats towards either the system in it self or the goal(s) it pursues. Following Mantovani [28], we define system identity as its core goals. The core goals are what the system holds as most central – this may of course be a continuum, with some goals being more important than others. The system should protect the core identity-defining goals, but be flexible with other goals. Those other goals may be instrumental to achieving or upholding core goals. Thus, opportunity may present itself in terms of recognition of new or novel ways of achieving core goals, adopting new instrumental goals, perhaps at the same time abandoning old instrumental goals. As systems are under pressure, the range of goals the system attempts to uphold may shrink.

During adverse circumstances, to uphold core goals (rather than abandoning them), may demand resilience. There are different conceptualizations in different areas of research, of what defines resilient systems, and of what core capacitates resilient systems have. In this paper, we include currently accepted core capacities from resilience engineering, as well as capacities recognized as important to crisis response and in some resilience engineering frameworks [see e.g. 29]. We choose to also include crisis response since cri-

ses represent circumstances that can present major adverse conditions to uphold core goals in previously well-adapted systems. Although, to other systems, that may previously have been ill adapted, the same situations may represent opportunity. Their core goals and abilities may match the new situation better than the old context did. We do not, in our model, consider systems resilient that were accidentally better suited for new situations. Resilience demands the intrinsic capacity to proactively or reactively adapt, while preserving core goals.

It is not uncommon in resilience engineering to refer to four processes of adaptation: Anticipating, Monitoring, Responding, and Learning, as for example in the case of the resilience cornerstones suggested by Hollnagel [30]. *Anticipation* stands for being able to, before the fact, take in the idea that a situation might occur, and to take action based on the prediction. *Monitoring* stands for the ability to detect, make sense of, and take action based on discovery of the onset of an event. *Responding* is the ability to take action during an unfolding event, whereas *Learning* stands for being able to adjust the system in the aftermath of an event, learning from both good and bad aspects.

Essentially, this is an example of an instantiation from a family of models which can be traced back to Neisser's perceptual cycle [31]. Similar models, such as Boyd's Observe-Orient-Decide-Act [32] or Hollnagel's Contextual Control Model [33] are also well-known examples of this cyclical arrangement of perception-understanding-action. Learning is not an explicit function in any of the mentioned models, but it is implicitly assumed, at least in the perceptual cycle and the Contextual Control Model that learning takes place. Otherwise the individual/organism that executes the cycle would be prone to committing the same mistakes again and again. It is thus fair to say that it is agreed that most purposeful organisms or systems need to fulfil these functions. Resilience is however not only dependent upon the ability to learn but also on the ability of the 'self' to recognize the need for change as well as be willing to change. As pointed out by e.g. [34-36], resistance to change in an organization is as an important factor when considering resilience, as is the willingness to change.

In contrast, in crisis, disaster, and emergency response, the following four abilities are often seen as central: mitigation, preparedness, response, and recovery [37, 38]. *Mitigation* stands for those activities oriented toward stability and risk avoidance, whereas *preparedness* regards future response activities. *Response* refers to being able to manage on-going events, and is also included in the cornerstones model described above. *Recovery* is about rebuilding, of bouncing back to where it was, or forward to where it would want to end up, in the short and long run.

In the following sections, we will present a holistic model of resilience, based on concurrent ideas in resilience engineering and crisis management. In contrast to previous frameworks, we propose a systemic model, highlighting dependencies between constraints, functions, and strategies.

The model consists of four different sections*; Event-based constraints*, *Functional Dependencies*, *Adaptive Capacity* and *Strategy*. Each sections aims to explain important aspects and properties of a resilient system. We start out by explaining and exemplifying event-based constraints, which are the contextual factors that the system must cope

with. We then present a set of core resilience functions, outlining functional dependencies for adaptive capacity between the functions. We also provide examples of resilience-critical properties of each function. Thereafter follows a section outlining functional dependencies that arise from coping strategies. The paper ends with a discussion about the proposed model.

3. EVENT-BASED CONSTRAINTS AS CONTEXTS FOR ADAPTATION

For any adaptive system, events present themselves as a *context for adaptation*. A resilient system is an adaptive system that protects its core goals, sometimes by sacrificing and replacing other goals that are instrumental to the core goals. This relates the system to unfolding, potential, or past events. The events are important for several reasons. As they unfold, they represent constraints, in particular related to time and space. Further, as threats, there may be a cost associated with dealing with them, which may result in the need to make trade-offs when deciding how to deal with them. It is of particular importance to notice that some core goals may become critical only in certain context, during particular kinds of events. Some systems may rely on hastily formed networks of organizations that do not collaborate during normal circumstances, but are formed in pursuit of some common core goal [39-41].

FIGURE 1. ABOUT HERE

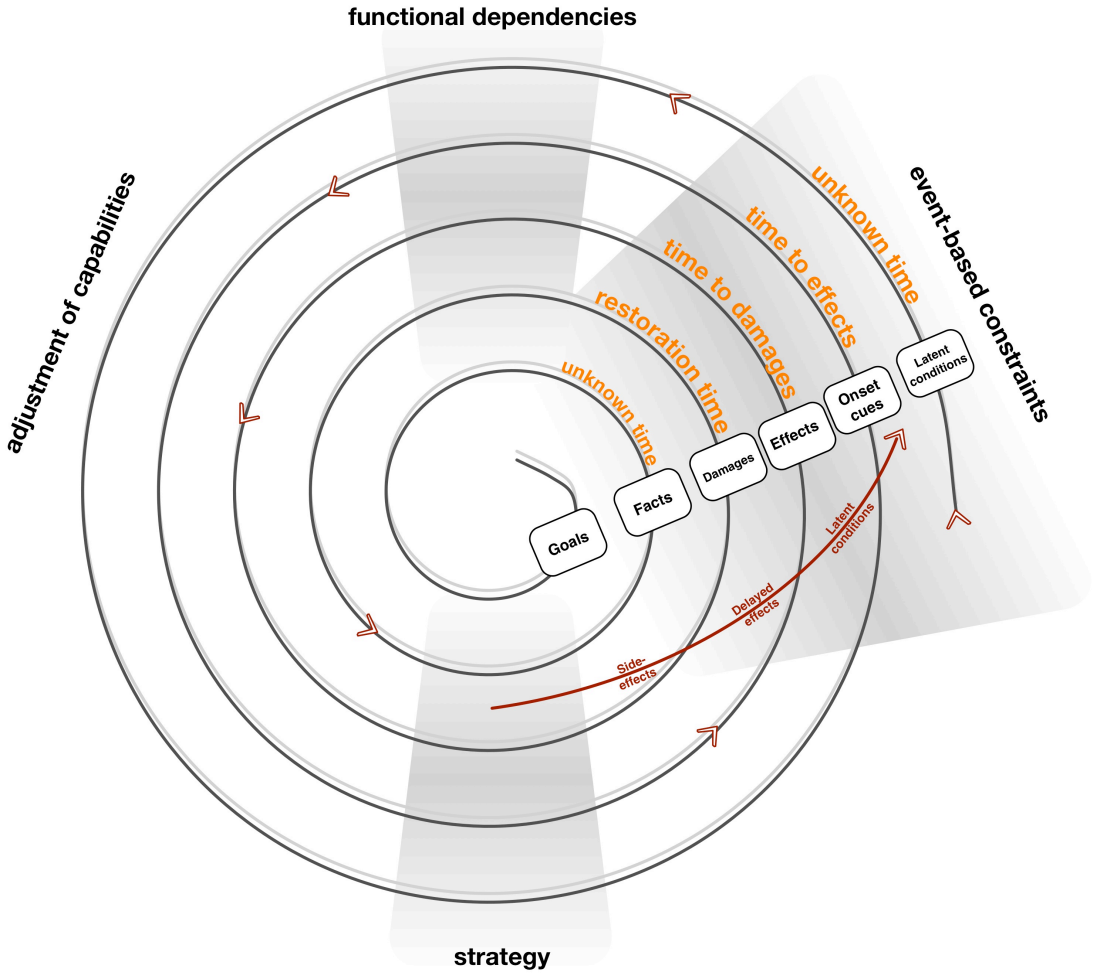

Figure 1. Event-based constraints.

Event based constraints (see Figure 1.) can be defined as *latent conditions* (vulnerabilities), *event onset cues*, *direct and indirect effects* of the event, and *damages* to the system. Indirect effects may be in the form of side effects of response or of damaged systems. The effects may be relatively direct, delayed, or causing new vulnerabilities rather than direct negative effects as new latent conditions.

It should be noted that although the model seemingly spirals inwards, it also spirals outwards, potentially forming complex feedback and feed forward loops. Firstly, partly or fully failed control may result in side-effects, delayed effects, and latent factors. Those effects spiral outwards. Side-effects appear one layer out, as new effects to manage during response. Delayed effects go yet another layer further out, as effects with an onset that may or may not be detected through onset cues. Latent effects, finally, are such that have no current momentum, but with effects that may be anticipated at the outer layer. Of course, the model also continues inwards, with direct effects of failed control, which may result in damage. This damage is something that may need to be recovered from. As events calm down, learning may be initiated to be better prepared in the future.

Example 1 – Power Grid Failures

Latent conditions, which may or may not be observable, are for instance aboveground electricity lines going through a dense forest. As no event has yet occurred that may cause the trees to fall over the lines, no particular time-related constrains are in play. *Event onset cues* for a storm may be in the form of increasing wind, or weather prognosis. The onset of an event may represent an opportunity for detection of the onset, but it also represent a constraint – time to the first effects of the event. Event *effects* are for instance trees that start falling in the strong wind. Those may cause damage immediately, but may also represent disturbances that can be dealt with without any particular effects. The presence of effects of the event usually represents both higher visibility (stronger cues) but also tighter constraints (e.g. less time to act). *Damages* may be *direct* such as falling trees cutting aboveground electricity lines, or by blocking roads. Damages represent new constraints, in particular with regard to time before the damages cause side effects potentially causing further damages. *Side effects* may also occur directly (no electricity), or be delayed (pumps failing in the waste-water system, causing overflow much later), or hidden as latent conditions (e.g. water eroding roads, but without collapsing them immediately).

Facing a major storm, a system may realign itself, into a crisis management mode, coordinating efforts from different actors more actively than during normal events. Representatives from different areas in a municipality may for instance form a crisis management team, to make sense of and coordinate efforts, to maintain core system *goals* (e.g. protect all their citizens).

Example 2 – Air Traffic Control

In Air Traffic Control (ATC), a *latent condition* in regular work is for instance wind and other factors that make performance of aircraft variable and somewhat unpredictable. As long as this performance variability does not combine with spikes from events, or other kinds of system variability, no particular event may become manifest. *Event onset cues* may be a slight change in speed or direction, compared to what was predicted or prescribed. *Effects* may be separation minima infringements, whereas *damages* may be rather direct and violent if separation is lost. Side-effects may furthermore stem from response, e.g. changing the speed, altitude or direction of an aircraft may cause new loss-of-separation events. Latent conditions may for instance emerge if an unusual occurrence (e.g. lack of runway lights) becomes an everyday occurrence, eroding the safety of the system. The events may threaten core system *goals* (e.g. safety through separation, and efficiency).

4. FUNCTIONAL DEPENDENCIES FOR ADAPTIVE CAPACITY

The upper part of the model (see Figure 2) describes functions that a system may employ to cope with events, and core functional constraints between them (to the left). The

six functions are arranged in a circular fashion, placing the functions where their output can be used at the earliest, in relation to events, thereby clarifying the relation between functional and event-based constraints. E.g. monitoring can result in event detection at the earliest after cues are present – but events may also be detected much later in which case the system is more constrained with regard to response. Thus, only the events per se unfold in a linear fashion. The functions are therefore not strictly coupled with any position versus event sequences. In figure 2, we emphasise this by hiding the spiral loop. E.g. anticipation may be a part of dealing with an unfolding event as well as something done well in advance. However, execution of the functions may be limited by event-based constraints. E.g. time constraints for organizing response are tighter if done during an on-going storm, compared to if they are done well before the storm has approached. Thus, both functional dependencies and event-based constraints affect the execution of the SyRes functions.

Below (Figure 2, left side, adjustment of capabilities), we also outline functional constraints on dynamically forming new functions. This is done through establishing and mobilizing modes. *Mobilization* represents actually getting resources deployed and active. *Establishing* represents deciding what the resources should do. Ideally, modes are first established, and then mobilized, maximizing the use of resources. In practice however, there may be a mix or even a reversed order. In particular, with high uncertainty of what has occurred, or of what side-effects might occur, mobilizing resources may be done before deciding exactly what functions they should perform.

FIGURE 2 ABOUT HERE

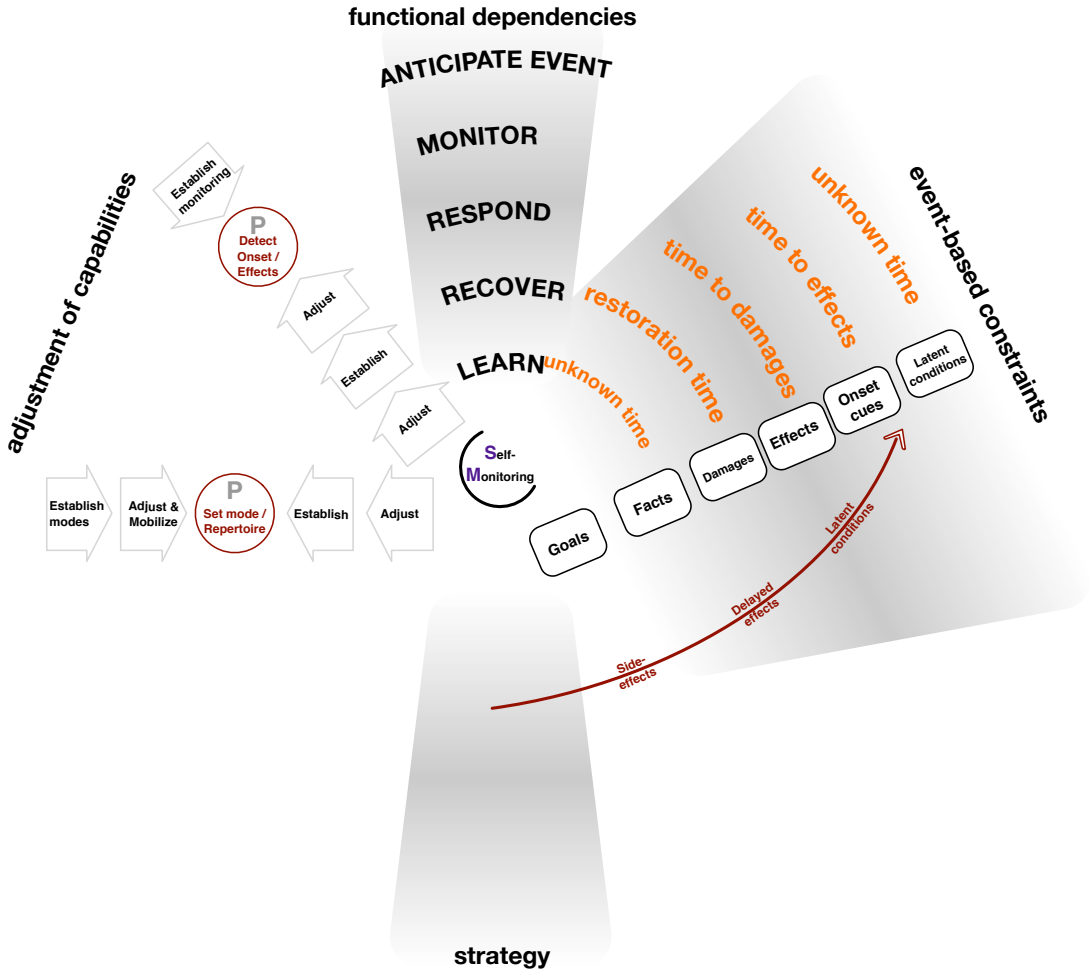

Figure 2. Functional dependencies and adjustment of capabilities

Requisite variety is a term used to describe the ability of systems to cope with situations [42]. Ashby's law states that only variety can destroy variety, i.e. when facing a dynamic situation, we must be able to respond before the situation gets out of hand. The term has previously been used to denote the capacity to understand what goes on (sensemaking variety), to affect what goes on (control variety), versus the variety of events that may occur (disturbance variety) [20]. Since in real life, the requisite variety may not always at every point in time precisely match what may occur, adaptive capacity becomes central. To meet previously unexpected or unplanned for events and circumstances, to change the variety of the system is then required. In real-life situations, it is thus important to differentiate between responses that can be initiated more or less right away, compared to responses that must first be envisioned and mobilized. In some cases major adjustments must be made during mobilization, in other cases the response is specified in detail in advance. For instance, in emergency response, there are (in Sweden) often very specific "canned" responses to specific lists of events, to be mobilized initially. That initial response is then adjusted in response to more information.

In our model *anticipation* is a pre-requisite for the ability of establishing, at the earliest point, functions for monitoring the onset of events, functions for event detection, preparing suitable modes of operation during response, and immunizing against threats that are completely avoidable. *Monitoring* is a pre-requisite for detecting the onset of events. Subsequently, abilities to detect effects of events may be adjusted and mobilized, response capabilities may be adjusted and mobilized, and effects may, in some cases, be entirely avoided by some manoeuvre. Initiating *response* is a pre-requisite for the ability to detect direct effects of events, respond to events through the current repertoire of action, to take control of events. Since damage may nevertheless occur, initiation of *recovery* is a pre-requisite for re-establishing damaged functions for detection of effects and damaged modes of operation. *Learning* is then a pre-requisite for adjusting functions for event detection and modes of operation, and feeds into the self-monitoring function at the centre of the model. Finally, at the core of this model, *self-monitoring* refers to the ability to monitor and adjust all other functions continuously, a pre-requisite for the ability to maintain the core abilities of the model. Whereas the sequential nature of unfolding events potentially trigger the functions in the model in such a way that it provides pre-requisites for adjusting its functionality against threats, self-monitoring describes the resilience of the system against threats to its intrinsic ability to adapt and respond, as a whole.

Anticipating

Anticipation, the expectations on what could potentially occur is crucial for detecting and coping with unwanted events. This function largely depends on *Requisite imagination,* a term coined by Westrum [43]. Requisite imagination refers to the ability to foresee/predict future problems – a skill that is very hard to assess in advance. Nonetheless, it is essential for preparedness – for the ability to adapt and adjust functions and processes in advance of events. Westrum describes three different event types: *regular, irregular* and *unexampled* events [43]. Regular events are well known, for example machine failure or bad weather. Irregular events are possible to imagine, but are normally so rare (or expensive to handle) that little specific preparation is taken. Earthquakes, large fires or chemical outlets are typically mentioned as examples of irregular events. Unexampled events are so rare that normally no organized mechanisms for coping with them exist, or could even be imagined. The 9/11 terrorist bombing or the flooding of New Orleans are often mentioned as examples of unexampled events. Events can also be considered with regard to familiarity and preparedness [44], into those that are routinely dealt with, those anticipated events that people nevertheless lack everyday experience of, and those that are unanticipated. For the second class of events, means may have been prepared, whereas the third class of events may require improvisation.

However, having specific capabilities of response versus specific threats are not exhibits in themselves of strong resilience, since new emerging threats may nevertheless later expose the system to new vulnerabilities. Thus, it is the active process of anticipation and adjustment that is the exhibit of resilience – rather than the adjustments per se. Both

adjustment of stability (e.g immunization) and adjustment of response capabilities (e.g. new response modes) may result from anticipation.

Anticipation is a pre-requisite for establishing modes of monitoring and modes of response, in advance of cues for the onset of events. The establishment of modes specifically tunes the requisite variety of the system, to make sense of and to control the specific anticipated events, or broader classes of events.

Example

Two situations from a previously published study [20], the Rune crisis response exercise, exemplify anticipation. The study evaluated how a small municipality in Sweden performed an exercise to prepare for future threats. The exercise focused on managing an irregular event, a storm, which is a threat that the municipality had previously faced. Successful anticipation was illustrated in dealings with the waste water system. Effects of power loss on pumps were anticipated, and response could be launched. In contrast, they failed to anticipate the effects of loss of electricity on telephone communications. In particular, they could not anticipate for how long the systems would be available after a loss of external electricity. Interestingly, in the fist case, resources needed for anticipation were already mobilized, present in the crisis management team. But in the second case, a new function was established and mobilized during a meeting. That process was however too slow to anticipate effects before they became actual effects.

Monitoring

Monitoring, the surveillance of crucial system parameters and events, is guided by anticipation. In most situations, we look for problems where we expect to find them. In technical systems, we install sensors and automation to cope with problems that we either have foreseen or learnt from experience that they are important. However, there is also another dimension to monitoring, namely the ability to interpret the signs of an upcoming problem once it is detected. *Requisite interpretation* [4, 5, 26] is a term used to illustrate the ability to recognize that something that goes outside of the routine means has actually occurred, and initiate, strengthen, or coordinate a process of adaptation in response to emerging events.

A particular problem for designing a monitoring function is that for less expected events it may be required to process data that rarely contain information that is needed, to interpret information that is rarely encountered, or even interpret common information in a new way. Firstly, to monitor for the less expected may become sacrificed during high workload (due to the need to monitor for more likely events). Secondly, during low workload, monitoring activity per se may be reduced, so that cues may not be encountered.

In Figure 2, having detected and taken in the actuality of the onset of an event is a prerequisite for adjusting and mobilizing response modes, based on onset cues. Although it

would certainly be possible to also the establish modes (what capacities are required) as a result of monitoring, on-going events then may constrain possibilities more severely than if modes are established based on anticipation. To actually make use of a monitoring function, resources must also be mobilized. However, for complex situations, monitoring functions only be partially mobilized at the outset, being mobilized more strongly as onset cues becomes present.

Example

In air-traffic control, specific monitoring support systems can be installed to support operators in monitoring for regular threats in the form of minimum separation infringements. For instance through tools such as Short Term Conflict Avoidance (STCA), and Medium Term Conflict Detection (MTCD). Although actual infringements are not that common, threats toward infringement occur frequently, and to manage them is a core aspect of the work of the controller. They are managed both through planning, and through adjusting traffic due to unpredictable conditions (E.g. it is in practice impossible to exactly predict the future position of an aircraft. It is always an approximation that is affected by numerous regularly present factors such as wind, as well as irregular factors such as aircraft system failure, resulting in deviations from predictions). The monitoring function, as embodied by the system of controller and automation has limits, e.g. due to the design of the automation presenting information on infringements and the speed of visual controller monitoring [45].

Thus, the system is highly optimized toward detecting regularly occurring threats in an efficient and effective way. Resources for responding to regular threats are also always mobilized – there is always both an active pilot and an active controller on duty in controlled airspace, and the traffic monitoring tools should always be online.

Responding

Anticipating and/or monitoring is/are needed in order to detect that something must be done in order to remain in control of a situation. The actual execution of actions is what prevents or mitigates the effects of anticipation/monitoring. In order to successfully act on a problem, there must be sufficient resources as well as the ability to coordinate those resources in a meaningful way to cope with the problem at hand.

Successful response, to control situations so that negative effects are avoided, requires (see Figure 2) the ability to detect particular effects of events, and to have suitable response modes (that may first have to be adjusted and mobilized). As figure 2 indicates, as soon as an event has been anticipated response capacity can be prepared and evaluated. However, as with all the functions, capacity may be mobilized much later, e.g. after the first damage has been done. But if executed later, event-based constraints are more severe. In particular, response through control may require mobilization of resources, since it may be impractical to be ready-to-act on every potential contingency at all

times. Mobilization may be severely constrained by events, e.g. since the physical distance between resources and events may cause considerable, and sometimes critical, delays.

Returning to what Westrum [43] called *regular*, *irregular* and *unexampled* events, it is clear that systems may be designed so that what occurs very often is mobilized, while what happens irregularly may require mobilization, and the unexampled may also require establishing capacities. Although this is not a strict rule, it shows that by design, systems may not have functions that are mobilized, ready to respond to every contingency at all times, e.g. due to the cost and effort involved, and due to the impossibility to anticipate every contingency. Nevertheless, some systems may be more specialized to one or the other kind of events. E.g., comparing Air Traffic Control (ATC), with Emergency Response (ER), and Crisis Response (CR) organizations, differences are apparent. Comparatively, ATC is more specialized in regular events, whereas ER is more concerned with irregular events, and CR is more specialized toward unexampled events.

Systems that need to be adaptive during response face an additional set of challenges compared to those that can rely on adaptation in advance of events. Firstly, to cope with side-effects of being resilient (see [23]), secondly to prepare structures for being resilient (see [22]). Furthermore, there is a problem of anticipating and detecting side-effects of adjustments that are made to cope with events [23]. Those side effects need to be differentiated from side effects from the response activities per se, for instance side effects from usage of chemical means to control an outbreak of insects.

An important observation is that side-effects also may appear, or rather be interpreted as, changes in the state of the situation that emerge from outside of the system rather than a side-effect of own actions. This may lead to a vicious circle of misunderstanding, where the actions taken generate more side-effects, which in turn distort the interpretation of what is happening – eventually leading to a situation where the system forms a positive feedback loop that only causes more confusion [46].

Further, for regular events, it may be possible to control events through regular line organizations. However, some large-scale events may rely on the formation of hastily formed networks of organizations. As pointed out elsewhere [40], a particular challenge for hastily formed networks is to establish conversation spaces. That includes both technologies and practices for communication.

Example

A debriefing on Swedish crisis response regarding two international missions revealed important insights on response, regarding side effects of re-assigning resources from one function to another. If a medical doctor, acting as manger, notices a lack of medical doctors and starts treat wounded, a side-effect may be delayed or omitted management action [23]. This may reflect the core goals of the system, to protect people, sacrificing the resilience of the system (an instrumental goal). However, to the extent that the event context is dynamic, the loss of resilience may later threaten the core system goals.

Recovery

In traditional crisis response and emergency response literature, it is common to refer to recovery as one of the four core activities [37, 38, 47]. Recovery refers to both short-term restoration, such as removing trees blocking roads, and to long-term restoration of destroyed infrastructure. What makes this central to resilience engineering is the notion in RE of "bouncing back", to recover from negative events that have occurred [11]. Although this may refer to response activities, it is also important to consider dealing with effects that have passed through layers of defence and caused damage [48].

It should be noted that as a notion of resilience, recovery should not merely be about bouncing back to how things were, but forward to a state that is well-adjusted to actual circumstances and foreseen threats, as seen during recovery. In "creative destruction", damaged parts are replaced by new constructs that have other abilities that are less damage-prone than their predecessors. Such forced design iterations are often an important driver for safety. In some respects this is an illustration of Safety I, especially when reconstruction focuses on immunization and increased robustness.

Successful recovery also refers to restoring functions facilitating resilience. During recovery, to bounce forward, new functions must be established, whereas to bounce-back previous functions need to be re-mobilized. Successful recovery may thus be a pre-requisite for continued response during events, as well as to regain or establish capacities after events.

Example

In Air Traffic Control, and in other high stakes domains, creative destruction can be exemplified by the replacement of one system generation by another. This usually not the result of any event damaging the system, but nevertheless exemplifies the removal of an old system, and the introduction of a new system. This old system may be left as a backup-system allowing recovery in case the new system malfunctions. The old system cannot be expected to support the same level of performance as the new system. Thus, recovery using the old system may result in graceful degradation of performance, rather than total system failure.

Learning

Learning is, and must be, a pre-requisite for any viable system. It is also central to resilience [30, 49]. If a system fails to learn from experienced events, negative or positive, it will spend unnecessary resources in all functions outside the learning part of the SyRes spiral the next time it faces the same or a similar event. Firstly, learning promotes the ability to monitor as it helps focusing attention. In some cases monitoring functions may even have been unavailable before an event has happened, but are introduced as an effect of the fact that the system has learned from its experience. There are numerous ex-

amples of this, such as earth-quake and tsunami warning systems that have been installed after severe events. Learning may thus be critical to bounce-forward after events, including learning from events that have affected other systems. In the same way, anticipation is affected. This may however not only be positive as events that have been experienced as significant can bias anticipation in a way that cannot be justified in terms of for example the actual likelihood of the same event.

Perhaps most importantly, learning helps the system improve its response to an event. By gathering and reflecting upon incidents, crises, and accidents, the system may improve its barriers and procedures for coping with an event or even re-configure its structures to better withstand known disturbances. Also, ways of applying recovery actions can be improved to better meet the demands and serve as a basis for a swift return to normal operations.

Learning is ideally a continuous function, at least from a resilience perspective, but in many real situations, learning emerges as a consequence of major disturbances, i.e. ad-hoc. Learning can therefore be based on feedback as well as feed forward. To prepare for resilience, it is important to capture conditions that have previously enabled local resilience. The system may then avoid that conditions for resilience are removed as a side-effect of other changes to the organization. Conditions may instead be strengthened and spread [22].

As has been reported previously [36], in accident investigation, the investigators often encounter resistance to their recommendations. They then (in practice, although not always explicitly) employ strategies to overcome the kind of resistance that they perceive. These strategies exemplify resilience of learning, rather than through learning.

In sum, the learning function can thus adjust the basis for detecting as well as actually be the basis for changing the existing repertoire/mode of control (see Figure 2).

Example

In practice, although humans may know their core goals, in organizations confusion may emerge. For instance, in a crisis response exercise that we have observed (see [20] for description of data collection methods), the participants re-discovered a central core goal. They realized, at one point, that since their core goal was to protect all their citizens that should also include those normally taken care of by private care giving organizations. They also observed that they had made the same omission before (indicating a lack of learning).

Self-monitoring

Recent research has shown that the ability to change may at times demand more than just having core abilities at some point in time – resilience may require the ability to

maintain the core abilities through adaptive processes during adverse conditions, in addition to preserving core system goals.

This problem is sometimes referred to as the Matryoshka problem [5] to emphasize that is a hard problem to tackle, since success cannot be guaranteed merely by using a new system to monitor the old system. The system is then vulnerable to that new system being damaged, and that system in turn then would need to be monitored. Although the problem is hard, perhaps impossible to completely solve, it presents a major challenge for systems that needs to be resilient.

As described in the example below, for instance in reflections by field staff on the Swedish crisis response missions after the Asian Tsunami of 2004, this problem was a major concern to the workshop participants [23]. In our model, we refer to this new, tentatively important ability of the system to monitor its core functions for resilience as *self-monitoring*. Without self-monitoring, all or individual core functions that facilitate resilience may deteriorate or even cease to function, seriously reducing the resilience of the system [23].

If a system, through self-monitoring, realize that it can no longer maintain its core resilience functions through the existing structures, it must find a way to transit those functions to a new structure, either by prepared measures, or by invention. As the system is a part of the environment in which it operates, it both shapes and is being shaped by the same environment. The self-monitoring function compares the value of success metrics (the effect of actions in the environment) with desired values, while reflecting upon its own resilience. If the current way of operating is deemed inappropriate, the system, based on its understanding of the situation, may chose to change its inner mechanisms to maintain success. Self-monitoring thus needs to be continuous versus change – with slow changes, continuity may be assured by self-monitoring at larger intervals. Self-monitoring may be a centralized or distributed process, executed before, after, or during events.

It is important to note that self-monitoring is not necessarily only driven by feedback during on-going events. In line with the definition of resilience engineering, the system may, based on its understanding chose to exploit circumstances or effect the environment based on anticipatory, feed forward driven, action. As represented through methods such as the Resilience Assessment Grid [50], self-monitoring may also be a systematic effort, assessing the system against core abilities.

Self-monitoring is thus qualitatively different from evaluating how the response work is progressing, and how (existing) functions of the system are (or should be) used. Further whereas learning is crucial in order to increase the performance repertoire of a system, self-monitoring is necessary in order to be able to maintain resilience both in the face of irregular and unexpected events, and to ensure that the core functions do not deteriorate with in adaptations during regular operations.

Example

Self-monitoring has been observed in crisis response, both as a bottom-up process and as a top-down process. As a bottom-up process, Swedish responders arriving at the scene of the Asian Tsunami of 2004 adjusted their roles to fit perceived needs. However, after this initial adaptive period, the ability of bottom-up self-organization was perceived as lost by responders who had participated in the event. It then depended on managerial action, which might also have been eroded if the manager had also taken an improvised role (away from management) [23]. Thus, self-monitoring is sometimes a distributed process, and at other times a centralized process.

STRATEGY

The execution of resilience functions may manifest in the form of basic *strategies* (Figure 3, lower part), e.g. *immunization* (moving a city from above a slowly collapsing mine, to a different location), *avoidance* (e.g. evacuation), *control* (e.g. attempting to control water flowing toward a city), *rebuilding* (e.g. repairing damaged buildings), or through *knowledge* (e.g. making sure every part of a community knows about threats and ways of coping).

FIGURE 3 ABOUT HERE

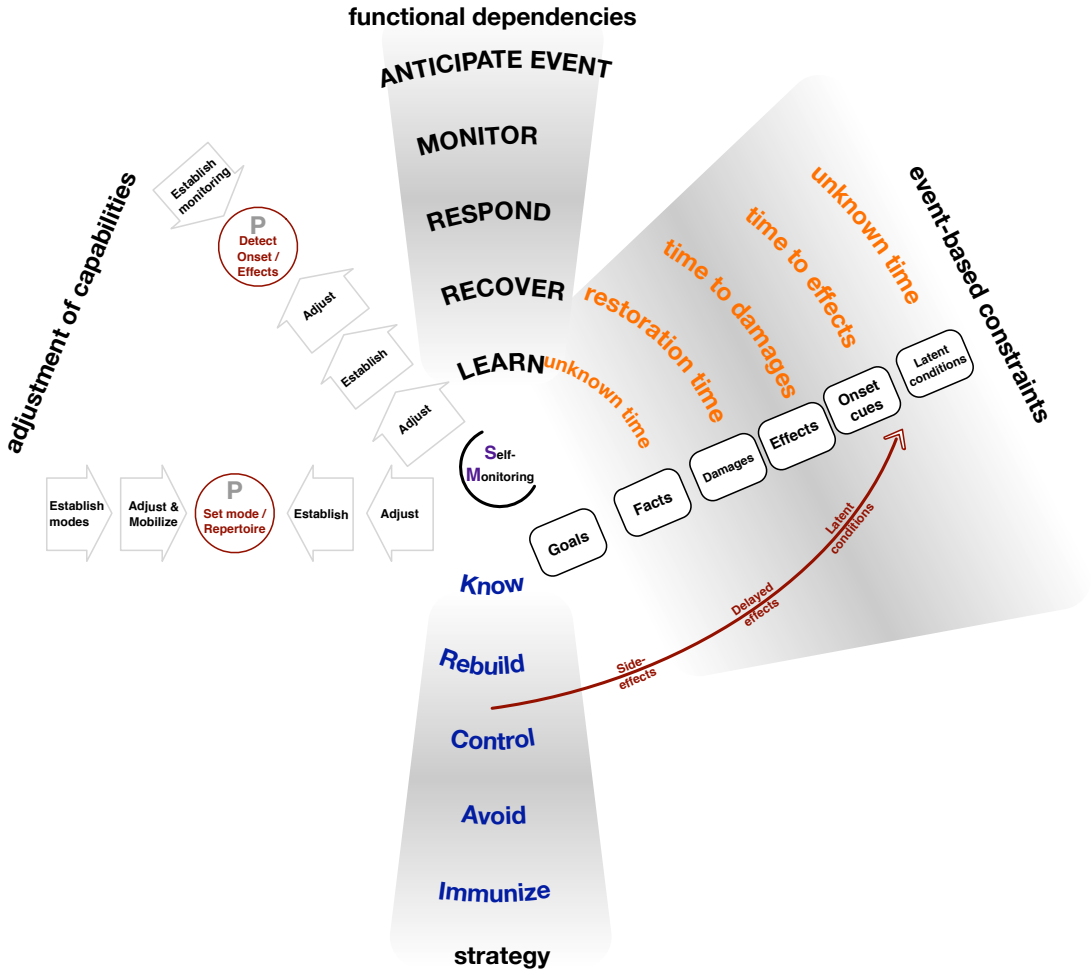

Figure 3. Strategy.

However, more importantly, resilience engineering may give rise to complex strategies that introduce additional functional constraints. For instance, a complex strategy may employ immunization (to a point), requiring monitoring (for what exceeds immunization), to deploy response (that may also work to a point), requiring capacity to rebuild (perhaps also during response). Different systems may employ different complex strategies, and within systems, different strategies may be employed to meet different threats. The particular strategies that are being engineered might for instance be modelled through some emerging framework such as Functional Resonance Analysis Method (FRAM) [51] or the Systems-Theoretic Accident Model and Processes (STAMP) [52].

Immunization

Successful *anticipation* should result in changes to the kind of events that the system should more or less routinely be able to cope with, by re-arranging its functions and resources permanently or through preparations for mobilization. In Figure 3, this corresponds firstly to *immunizing*, to make the system immune to the threat, for instance by

moving out of harms way (e.g. moving an entire city from above a collapsing mine to solid ground, as in the case of the Swedish city Kiruna which is being moved to a new location as a consequence of the extensive mining in the area).

Immunization may in many cases only be partial. A system might be immune to effects only up to a point, which may lessen the impact of events, even when the limits have been passed. This then represents a *shock absorber*. A differentiation can be made between shock absorbers that degrade gracefully when limits have been passed, and those that on the other extreme rapidly collapse. In both cases, the system gains time, to detect and react to the on-going event, but in the second case, a stronger response is needed more rapidly to cope. Immunizing, which is arguably the strongest strategy, is not always achievable. The system may then adjust its ability to *a) detect and make sense of* the onset of events (monitoring), *b)* adjust and prepare *modes of operation* that can be mobilized after detection, *c)* adjust the *response capabilities* per se, necessary to act during response.

Avoidance

In cases where an anticipated event cannot be immunized against, to avoid what is coming may nevertheless be an option, if the *monitoring-function* detects the event in time. If there is insufficient time to eliminate the threat by immunization, other measures may be taken to cope with it, such as moving out of harms way in a more immediate way than in the case of immunization. For example, a building may be evacuated in the case of a fire because a smoke detector triggers an alarm (the monitoring function detected the event) rather than making the building immune to fires. *Avoidance* may thus be an elaborate strategy, based on the assumption that it either isn't possible to make something immune or that it is too expensive.

A Tsunami warning system is a good example of an avoidance strategy – it is to difficult/expensive/impractical to make a coast line immune to Tsunamis, but the problem can be at least partly avoided given that a monitoring function exists that can provide an early warning.

Avoidance strategies thus strongly depend on effective monitoring functions, which also may be complemented by shock absorbers (partial immunization), reducing the need for high sensitivity of the monitoring functions.

Control

There are cases where it is both impossible to fully immunize against, and to fully avoid a situation. Sometimes this is because the situation was detected too late or because the onset cues where not interpreted correctly. In cases where a problem cannot be avoided, it must be dealt with. One approach is to attempt to control it, or to control its effects. The *response-function* decides in what way control should be exercised, i.e., what kind

of actions that should be taken to assure that the situation does not escalate into an undesirable state. A typical example can be the creation of temporary barriers to control flooding in order to avoid damage to housing or water-bomb areas to prevent a forest fire from spreading. However, it should be noted that most control actions have side-effects, both in positive and negative respects. Controlling a flood by the construction of barriers may for example worsen the problem for residents in other areas.

Control may also, just like avoidance, be a deliberate strategy, as there are situations where problems may be anticipated, but impossible or impractical to immunize against. If neither avoidance, nor immunization strategies are used, the functional dependency to monitoring may be event stronger for response as a deliberate strategy against events– in particular for events demanding extensive mobilization.

Further, when relying on control to manage situations that are otherwise unprepared-for, anticipation or learning may nevertheless be important. Rather than preparing for the particular, control may be dependent on learning or anticipating particular success factors or vulnerabilities. For instance, returning to the case of the Swedish response teams, preparations that made people prepared to take improvised roles, in general, was seen as important [23].

Re-building

Naturally, there are cases where immunization, avoidance and control fails and damage is caused to a system. In such cases, systems may still prevail by adapting a re-building strategy as a way of re-taking what has been lost. It should be noted that this not necessarily mean that what has been damaged must be re-built in the same way as it was. In some cases, such as with regard to approaching storms, re-building may be a critical strategy, since some direct effects of storms cannot be blocked, avoided, or controlled.

Re-building may also be a deliberate strategy – to allow events to destroy a system, being prepared to rebuild it afterwards. It may also be a partial strategy, focussing response on some parts of a system, and focussing preparations for rebuilding on other parts, that are planned to be sacrificed in case of an event. If re-building is used as a deliberate strategy, it may depend on monitoring, to be able to initiate preparations event before the full onset of events.

High Reliability Organizations rely on rebuilding, to maintain functionality of their own system. It is achieved through redundancy, e.g. of staff being multi-competent through rotating crew positions, and through being assigned as back-up for other functions, a redundancy strategy called “Stressing-the-survivor” [53].

Knowledge

The creation of knowledge from learning is something that holds the potential for increasing the resilience of a system. This comes both in the form of better pre-requisites for anticipating, monitoring, responding and re-building. It can be seen as a strategy in the sense that an explicit process for learning can exist within the system, providing structure for gathering important information, in contrast to learning by "chance". This is a well-recognized feature in many high-reliability organizations where learning strategies are explicit and encouraged [53]. Incident and accident reporting systems are examples of such efforts, as are learning from exercises.

As a strategy, knowledge may be used for instance as a source for improvisation. Having experiences from real or trained situations, this knowledge may be used to improvise – even if there have been no explicit advance preparations for the specific courses of actions. Thus, knowledge is particularly central for systems operating in environments with high uncertainty. Returning once again to the Swedish Response Teams, a strategy suggested was to use learning on-site, to use periods of low workload to teach each other how to work in the own specialist role [23]. Other functions may thus depend on knowledge as a deliberate strategy.

6. DISCUSSION

As pointed out in the beginning of this article, there are many definitions and uses of the terms "resilience" and "resilience engineering". Although being useful in themselves, no systemic framework for applying the terms have existed. Our answer is the SyRes model (Figure 4.).

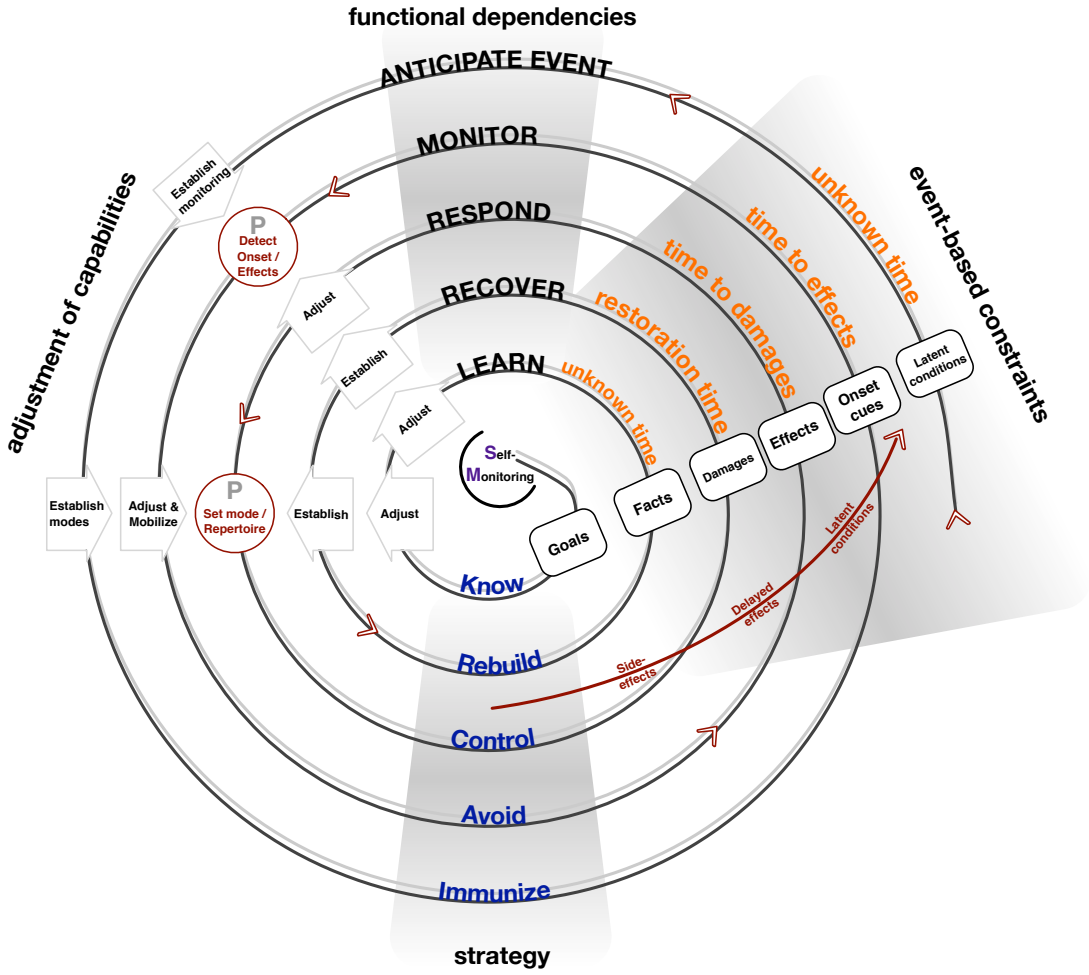

Figure 4. The SyRes model.

The model includes traditional Safety I principles, such as immunizing towards danger, or avoiding it. However, with regard to these principles, the model focuses on how to make sure they are current (e.g through anticipation and learning), adjusting and changing them to match current treats (by learning and self-monitoring), hence resilience/Safety II. Thus, the model describes resilient robustness, resolving the apparent contradiction between resilience definitions, in line with the challenge posted by Johansson & Lundberg [4], who stated that the challenge of the resilience engineer is to balance stability-enhancing properties (Safety I) with resilience-enhancing properties (Safety II) when designing a system. There are thus some important features of a safe/resilient system that is illustrated in the model. The system must be able to bounce back, with regard to maintenance of core goals, while being flexible with regard to instrumental goals:

- With strong anticipation, the system may on the one hand be resilient through strengthening its defences, using traditional safety I principles, but constantly reassessing threats and revising the principles. On the other hand, it may also re-

vise its means for response, minimizing the need for flexibility and adjustments during response.

- With strong monitoring, the system may exhibit resilience through effective deployment of prepared means, or through rapidly and flexibly devising and deploying responses based on the event.
- With strong response, the system may exhibit resilience through improvisational ability, to rapidly adjust the use of resources at hand (within time constraints and other acute constraints). The system may devise, deploy and respond at the same time.
- Having strong capacity for recovery, the system may restore its abilities to uphold core goals, through restoration of what corresponds to previous instrumental goals, or new instrumental goals. At times, it may also engage in creative destruction, in taking down a system that works, to replace it with one that works better.
- Finally resilience may refer to self-monitoring, the ability to adjust and maintain the core resilience functions. It is vital to recognize that resilience per se may be lost, either accidentally or as the result of a deliberate trade-off during adaptive behaviour that is otherwise beneficial to uphold core system goals. Resilience loss during adaptive behaviour is a potential vulnerability that a strong self-monitoring function aims at addressing

Thus, the model resolves the apparent contradictions between being well-prepared and agile during response, or bouncing back / forward after an event. A system may be resilient with respect to all the facets of the model – or may be evaluated or prove to have strengths in some area while being vulnerable in another. Therefore, when speaking of resilience, it can be helpful to state with respect to what parts of the SyRes a system is resilient, or has exhibited resilience.

On the whole, the model primarily emphasizes safety II, and the hard work of keeping a system resilient through the six facets of the SyRes model. In particular, the model highlights constraints – emerging from the context, from particular functions, and from deliberately engineered strategies for resilience. A consequence of using the model, and thereby understanding the dependencies between constraints, functions and strategies is that it becomes apparent that focusing/investing in certain strategies affects to what constraints that can be dealt with, and what resilience functions that need to be developed. Also, the constraints will shape what functions and strategies that a system should focus on maintaining. However, when pursuing resilience, it should always be remembered that an appropriate balance in terms of investment in different strategies is the most viable solution when facing uncertainty and situation dynamics, as it per definition is impossible to identify all possible situations that a system may have to cope with.

It will be a great challenge to the safety and resiliency community to develop running indicators of whether this resilience-related activity is active, in the absence of events that will be captured by regular Safety I principles. With regard to crisis response, the corresponding challenge is to keep running indicators of the agility and strength of core

resilience functions, in the absence of actual crises. The successful management of a crisis (or crisis exercise) does not mean that there is a resilient system in place – the learning functions must also be tested, and it must be assured through running resilience indicators that resilience does not erode. If it does erode, due to lacking or insufficient self-monitoring, without functioning resilience, resilience per se might not recover. The Matryoshka problem, as described by Lundberg and Johansson [5] states that no system can be perfectly safe or resilient, as the functions that are created to monitor safety/resilience in them selves need to be monitored, creating a, theoretically, infinite chain of monitoring functions.

Due to the Matryoshka problem and the occurrence of unexampled events, we can never create a system that is completely safe or resilient. However, we can strive towards maximizing the resilience of each system that we in practice can affect. Although the problem cannot be completely solved, it is nevertheless an important facet to design, engineer, or measure. As noted by Holling [6] some systems are hard to push over the boundary, but when they do, the state change may be very hard to reverse. Loss of resilience may be such a state change, since there is then no active function attempting recovery.

It is a major challenge to engineer a system so that a state change from having a resilient system to the loss of the core resilience functions (Figure 2) hard to achieve, but easy to reverse. To arrange in advance for the re-emergence of lost core resilience functionality in a system may prove to be unachievable, but is nevertheless a challenge with great reward if met. Of even greater challenge and reward is the design of emergent resilient systems in a community at large, to protect the community, from a multitude of systems regularly concerned with other tasks. As previous research has illustrated, practical methods can be both be built and assessed based on theoretical models. Our contribution, the SyRes model, is therefore central to evaluate that methods are up to date, and to stand at the core of novel methods.

REFERENCES

[1] Karwowski W. A Review of Human Factors Challenges of Complex Adaptive Systems: Discovering and Understanding Chaos in Human Performance. Human Factors: The Journal of the Human Factors and Ergonomics Society. 2012;54:983-95.

[2] Checkland P. Systems Thinking, Systems Practice:. Chichester: Wiley; 1999.

[3] Hollnagel E. A tale of two safeties. Nuclear Safety and Simulation. 2013;4:1-10.

[4] Johansson B, Lundberg J. Engineering Safe Aviation Systems: Balancing Resilience and Stability. In: Wise JA, Hopkin D, Garland DJ, editors. Handbook of Aviation Human Factors. 2nd ed. Boca Raton, FL: CRC Press; 2010.

[5] Lundberg J, Johansson B. Resilience, Stability and Requisite Interpretation in Accident Investigations. In: Proceedings of 2nd Resilience Engineering Symposium Juan-les-Pins, France: November 8-10; 2006. 191-8.

[6] Holling C. Resilience and stability of ecological systems. Annu Rev Ecol Syst. 1973;4:1-23.

[7] Patterson ES, Woods DD, Roth EM, Cook RI, Wears RL, Render ML. Three Key Levers for Achieving Resilience in Medication Delivery with Information Technology. Journal of Patient Safety. 2006;2:33-8.

[8] Bosher L. Built-in resilience through disaster risk reduction: operational issues. Build Res Inf. 2013;42:240-54.

[9] Wildavsky A. Searching for Safety. New Brunswick, N.J.: Transaction Publishers 1988.
[10] Davoudi S, Shaw K, Haider LJ, Quinlan AE, Peterson GD, Wilkinson C, et al. Resilience: A Bridging Concept or a Dead End? "Reframing" Resilience: Challenges for Planning Theory and Practice Interacting Traps: Resilience Assessment of a Pasture Management System in Northern Afghanistan Urban Resilience: What Does it Mean in Planning Practice? Resilience as a Useful Concept for Climate Change Adaptation? The Politics of Resilience for Planning: A Cautionary Note. Planning Theory & Practice. 2012;13:299-333.
[11] Manyena SB. The concept of resilience revisited. Disasters. 2006;30:434-50.
[12] Hollnagel E. Resilience engineering and the built environment. Build Res Inf. 2013;42:221-8.
[13] Hornell JF, Orr JE. Assessing behaviors that create resilient organizations. Employ Relat Today. 1997;24:29-39.
[14] Comfort LK, Boin A, Demchack CC. The Rise of Resilience. In: Comfort LK, Boin A, Demchack CC, editors. Designing Resilience: Preparing for extreme events. Pittsburgh, PA: Univeristy of Pittsburgh Press; 2010. p. 1-12.
[15] Longstaff PH, Koslowski TG, Geoghegan W. Translating resilience: a framework to enhance communication and Implementation. In: 5th Resilience Engineering Association Symposium Soesterberg (The Netherlands): 25 – 27 June 2013; 2013. 1-8.
[16] Mendonca D, Wallace WA. Adaptive Capacity: Electric Power Restoration in New York City Following the 11 September 2001 Attacks. In: Proceedings of 2nd Resilience Engineering Symposium Juan-les-Pins, France: 8-10 November; 2006. 209-19.
[17] Vale LJ. The politics of resilient cities: whose resilience and whose city? Build Res Inf. 2013;42:191-201.
[18] Lundberg J, Rankin A. Resilience and vulnerability of small flexible crisis response teams: implications for training and preparation. Cognition Technol Work. 2013:1-13.
[19] Rankin A, Lundberg J, Woltjer R. Resilience Strategies for Managing Everyday Risks. Proceedings of the 4th Resilience Engineering Symposium. Sophia Antipolis, France2011.
[20] Lundberg J, Törnqvist E, Nadjm-Tehrani S. Resilience in Sensemaking and Control of Emergency Response. Int J Emergency Manage. 2012;8:99 - 122.
[21] Lundberg J, Woltjer R. The Resilience Analysis Matrix (RAM): Visualizing functional dependencies in complex socio-technical systems. In: 5th Resilience Engineering Association Symposium Soesterberg (The Netherlands): 25 – 27 June 2013; 2013.
[22] Rankin A, Lundberg J, Woltjer R, Rollenhagen C, Hollnagel E. Resilience in Everyday Operations: A Framework for Analyzing Adaptations in High-Risk Work. Journal of Cognitive Engineering and Decision Making. 2014;8:78-97.
[23] Lundberg J, Rankin A. Resilience and vulnerability of small flexible crisis response teams: implications for training and preparation. Cognition Technol Work. 2014;16:143-55.
[24] Trnka J, Johansson B. Resilient Emergency Response: Supporting Flexibility and Improvisation in Collaborative Command and Control. In: Jennex ME, editor. Crisis Response and Management and Emerging Information Systems: Critical Applications Hershey, PA: IGI Global; 2011. p. 112-38.
[25] Woltjer R, Trnka J, Lundberg J, Johansson B. Role-Playing Exercises to Strengthen the Resilience of Command and Control Systems. In: Proc of the 13th European Conference on Cognitive Ergonomics (ECCE) – Trust and Control in Complex Socio-Technical Systems Zurich, Switzerland: September 20 - 22, 2006; 2006.
[26] Lundberg J, Johansson B. Pragmatic Resilience. In: Resilience Engineering Workshop Vadstena, Sweden: 25–27 June, 2007; 2007. 37-42.
[27] Lundberg J, Rollenhagen C, Hollnagel E. What-You-Look-For-Is-What-You-Find - The consequences of underlying accident models in eight accident investigation manuals. Saf Sci. 2009;47:1297-311.
[28] Mantovani G. New Communication Environments: From Everyday to Virtual. London, Bristol PA: Taylor & Francis 1996.
[29] Becker P, Abrahamsson M, Tehler H. An Emergent eans to Assurgent Ends: Societal Resilience for Safety and Sustainability. In: Nemeth C, Hollnage E, editors. Resilience Engineering in Practice, Volume 2 - Becoming Resilient. Surrey, UK and Brurlington VT: Ashgate; 2014.
[30] Hollnagel E. The Four Cornerstones of Resilience Engineering. In: Nemeth CP, Hollnagel E, Dekker S, editors. Resilience Engineering Perspectives: Preparation and Restoration. Burlington, VT: Ashgate; 2009. p. 117-33.
[31] Neisser U. Cognition and Reality: Principles and implications of cognitive psychology. San Fransisco: W H Freeman and Company; 1976.
[32] Hammond GT. The Mind of War: John Boyd and American Security. Washington, DC: Smithsonian Institution Press; 2001.

[33] Hollnagel E. Human reliability analysis: context and control. London, UK: Academic Press; 1993.
[34] Farrell PSE, Connell D. Organizational agility. In: 15th ICCRTS: The Evolution of C2 Santa Monica, California: June 22-24; 2010.
[35] Dijkstra A. Safety Management in Airlines. In: Hollnagel E, Woods DD, Leveson N, editors. Resilience engineering: concepts and precepts. Aldershot: Ashgate; 2006. p. 183-203.
[36] Lundberg J, Rankin A, Rollenhagen C, Hollnagel E. Strategies for dealing with resistance to recommendations from accident investigations. Accid Anal Prev. 2012;45.
[37] McLoughlin D. A Framework for Integrated Emergency Management. Public Administration Review. 1985;45:165-72.
[38] Altay N, Green Iii WG. OR/MS research in disaster operations management. European Journal of Operational Research. 2006;175:475-93.
[39] Denning P. Hastily formed networks. CACM. 2006;49:15-20.
[40] Lundberg J, Törnqvist EK, Nadjm-Tehrani S. Establishing conversation spaces in hastily formed networks: the worst fire in modern Swedish history. Disasters. 2014;38:790-807.
[41] Healey MP, Hodgkinson GP, Teo S. Responding Effectively to Civil Emergencies : The Role of Transactive Memory in the Performance of Multiteam Systems. In: Proceedings of NDM9, the 9th International Conference on Naturalistic Decision Making London: June 23-26; 2009. 53–9.
[42] Ashby WR. An introduction to cybernetics. London: Chapnam & Hall; 1956.
[43] Westrum R. A typology of Resilience Situations. In: Hollnagel E, Woods D, Leveson N, editors. Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate; 2006. p. 55-65.
[44] Vicente K, Rasmussen J. Ecological interface design: theoretical foundations. Systems, Man and Cybernetics, IEEE Transactions on. 1992;22:589-606.
[45] Lundberg J, Johansson J, Forsell C, Josefsson B. The Use of Conflict Detection Tools in Air Traffic Management – an Unobtrusive Eye Tracking Field Experiment During Controller Competence Assurance. In: HCI-Aero 2014 - International Conference on Human-Computer Interaction in Aerospace Silicon Valley, California, USA: July 30-August 1 2014; 2014.
[46] Hollnagel E. Context, cognition and control. In: Waern Y, editor. Co-operative process management: cognition and information technology. Bristol, UK: Taylor & Francis; 1998. p. 27-52.
[47] Galindo G, Batta R. Review of recent developments in OR/MS research in disaster operations management. European Journal of Operational Research. 2013;230:201-11.
[48] Birkland T, A., Waterman S. Challenges of Disaster Resilience. In: Nemeth CP, Hollnagel E, Dekker S, editors. Resilience Engineering Perspectives: Preparation and Restoration. Burlington, VT: Ashgate; 2009. p. 15-69.
[49] Comfort LK, Namkyung O, Ertan G, Scheinert S. Designing Adaptive Systems for Disaster Mitigation and Response: The Role of Structure. In: Comfort LK, Boin A, Demchack CC, editors. Designing Resilience: Preparing for extreme events. Pittsburgh, PA: Univeristy of Pittsburgh Press; 2010. p. 33-61.
[50] Hollnage E. Epilogue: the resilience analysis grid. In: Hollnage E, Pariès J, Woods D, Wreathall J, editors. Resilience Engineering in Practice - A guidebook. Farnham, UK: Ashgate; 2011. p. 275–96.
[51] Hollnagel E. FRAM: The Functional Resonance Analysis Method - Modelling Complex Socio-technical Systems. Farnham, UK: Ashgate; 2012.
[52] Leveson N. A new accident model for engineering safer systems. Saf Sci. 2004;42:237–70.
[53] Rochlin GI, Porte TRL, Roberts. KH. The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea. Naval War College Review. 1987;40:76-90.