Exploiting Latent Functional Capabilities for Resilience in Design of Engineering Systems

Abstract:

In this paper, we address latent functional capabilities, capabilities that were neither intended nor recognized in the design process. We propose that latent capabilities can improve the resilience of engineering systems, enabling recovery of performance after disruptive events. Engineering systems are designed to meet their functional requirements, and have a limited ability to avoid critical failures. Normally, redundancies are put in place to reduce the impact of potential disruptions, adding to cost and complexity. An alternative is to uncover latent capabilities that can be used to recover from disruption by altering the function-form mapping. Existing design methods focus on intended, manifest functionality, and do not consider latent capabilities. With basis in design theory, we show that latent capabilities can enhance resilience, and demonstrate this using two illustrative cases. Further, we propose approaches to uncover latent capabilities in systems design, and discuss implications of using latent capabilities to enhance resilience.

Keywords:

Resilience, latent capabilities, engineering systems, design theory, axiomatic design

1. Introduction

Engineering systems are designed towards meeting a set of functional requirements. Latent functional capabilities exist when engineering systems have the ability to perform functions that were not thought of during the design process, that often remain hidden even during operation. We investigate what happens when complex engineering systems lose the ability to perform their functions, and propose that latent functional capabilities can be used to increase embedded system resilience, acknowledgning that not all unwanted events can be avoided. Normal accident theory (Perrow 1999) points out that some hazardous events are impossible to predict and prevent, due to complex interaction between tightly coupled system components. The consequences of these events escalate beyond what could be imagined at the time of the initiating event, suggesting that there is an inherent difficulty in identifying and quantifying every important causal link (Klinke and Renn 2002). Complex systems theory explains that interrelations between components in complex engineering systems follow a power law distribution (Newman 2005), meaning that the systems are robust to disturbances at most system components, while extremely vulnerable to disruptions of the most highly connected components (Cohen et al. 2000; Albert et al. 2004). Hence, as the structure of most engineering systems are not fully understood, designers need to proactively consider how systems can be enabled to recover from events that disrupt functioning and degrade system performance, supplementing design strategies based on risk management with resilience (Park et al. 2013). In other words, designers should design resilience into engineering systems, embedding systems with the ability to recover in the aftermath of a disruption.

The design process maps from the functions the system is intended to perform to satisfy some need, to a physical description of a system. Pahl and Beitz (1996) divides the process into task clarification, conceptual, embodiment, and detail design, and suggests that a functional structure be derived, and mapped to the physical space by selection of appropriate working principles. For a precise mathematical theory of the open-ended, abductive design process, we refer to Braha and Reich (2003). Axiomatic design proposes two design axioms that we should follow to produce good designs (Suh 1990). First, design should adhere to the Independence Axiom, which states that functional requirements must be independent, to avoid functional coupling. Second, design should adhere to the Information Axiom, by minimizing the information content needed to describe the design, signifying a reduction of complexity (Kolmogorov 1983). Suh (1999) separates two distinct complexities for axiomatic design; real and imaginary complexity, where the real complexity represents the information content, and the imaginary complexity arises when the designer has a

limited understanding of the system itself. Addressing design complexity, Braha and Maimon (1998) refer to functional complexity as the probability of successfully meeting functional requirement. They define structural complexity as the number of components and interfaces in the system.

The design process completes when the proposed form meets the stated needs and requirements. At this point, there are typically additional undiscovered capabilities in the non-primary function-form mapping. This is especially true for the design process of complex engineering systems (Park et al. 2013). Following Merton (1968), we separate manifest functions designed intentionally into the system from latent functions. Manifest functions represent the initial intentions of the system, or its "*objective consequences*" resulting from the function-form mapping of the original design process. On the other hand, latent functions are "*neither intended nor recognized"*, and exist as byproducts of the intentions of the designers. Crilly (2010) proposes a scheme for analyzing the technical, social and aesthetic functions of artifacts. One of the dimensions in this scheme is the distinction between manifest and latent functions. The degree to which the function of a product is latent, depends on the stakeholder considered. Product functions that are latent to the designer can be manifest to the user, and vice versa. If product users cite several different purposes for one product, the product is likely to be valued higher due to functions that are latent to the designer (Crilly, 2010). Ross and Rhodes (2008) use latent value as a term describing desirable system properties that are not explicitly articulated during the design process. They propose that latent values can be elicited by altering the cognitive frames designers use to define the problem, as the framing of the problem creates biases that affect design choices (Tversky and Kahneman 1981). Sutcliffe and Vogus (2003) point out that latent organizational resources can be activated as the system context changes due to new challenges, for example disruptions.

Madni and Jackson (2009) present functional redundancy as one of numerous design principles that are meant to lead to resilient systems. Functional redundancy exists when different components have the ability to perform the same function. Hence, functional redundancy is different from physical redundancy, which is based on the parallelization of components making it possible for one component to fail without severe consequences for the overall system performance (Rausand and Høyland 2004). Physical redundancies are often included in a system to increase reliability, but can be hard to justify as these are mainly seen as cost-drivers. The value of physical redundancies only becomes apparent once failure occurs. From the perspective of resilience, one should hence seek to apply functional redundancies rather than physical redundancies to as large an extent as possible (Madni and Jackson 2009). Even though functional redundancy may come at a more favourable cost than designing physical redundancy into the system, functional redundancy implies an increased load for components that step in to provide functionality. The limited capacity of every system component to carry additional loads, represent a constraint on the use of functional redundancy (Braha and Bar-Yam 2007).

A distinction should also be made between latent functional capabilities, and concepts like multi-modality in products. Liu et al. (2015) discuss multi-modality in product design, decomposing into technological multi-modal design, and functional multi-modal design. Liu et al. (2015) define modes as switchable configuration states made for the purpose of providing specific functions or technologies. In the case of NASA's New Horizon mission, the dish antenna was used not only for its primary function of data transmission. It also acted as a protective shield against space debris (Stern 2015). Hence, depending on its positioning, the spacecraft exhibited several functional modes. The protective functional mode could be an example of a latent capability, if this functioning was not planned ahead of launching the system. What then distinguishes latent capabilities for resilience from functional redundancy and multi-modality is the degree to which the designer intended a system component to perform a specific function during the design process.

This paper takes the position that resilience in engineering systems can be enhanced by uncovering and exploiting latent functional capabilities in the design. We narrow the scope of the paper to concern how the system can recover from internal failure modes by altering its function-form mapping. Further, we suggest a methodology for identifying and planning for the use of latent capabilities to recover system functioning after failure. Two illustrative case studies are provided to show that latent capabilities provide systems with the resources needed to recover from failure modes improves resilience. We also discuss implications for axiomatic design, and the limitations of using latent capabilities relating to overall system performance, regulations, and the ability of an organization to enable adaptation of the function-form mapping.

2. Defining and measuring resilience

2.1. Reviewing resilience definitions

Resilience is a temporal lifecycle property of engineering systems (de Weck et al. 2011). The use of resilience as a term to describe the ability of a system to persist change originates in ecology (Holling 1973). Wildavsky (1988) uses resilience to describe strategies for reorganization of resources to respond to threats after they occur, enabling the system "*to bounce back"* from disruption. Much of the literature on resilience applied to engineering systems, including supply chains, came into being as a response to numerous events that disrupted the operation of complex engineering systems in the late 1990's and early 2000's. Common examples include the Kobe Earthquake in 1995 which destroyed much of the city's port capacity, a fire at a New Mexico factory which disrupted the production of Nokia and Ericsson phones, the 9/11 attacks, and the 2004 Indian Ocean earthquake and tsunami (de Weck et al. 2011; Park et al. 2013).

As resilience is studied in many disciplines, researchers have pointed out the lack of a common definition (Sheard and Mostashari 2008; Woods 2015; Hosseini et al. 2016). Some even argue that the term may become meaningless as a consequence of this lack of clear definition (Lundberg and Johansson 2015; Mekdeci et al. 2015). Reasons for this lack of coherence are the underlying differences in the scope of analysis, with respect to time periods chosen, the system boundaries, the disruptive events considered, the actions suggested for coping with the disruption, and the system qualities that should be preserved (Sheard and Mostashari 2008). Similarly, Woods (2015) distinguishes between four separate concepts all labeled resilience. This lack of commonality shows the importance of clearly defining what is meant by resilience whenever the term is used. For this reason, we review a number of resilience definitions, and metrics that have been suggested for quantification of resilience.

Asbjørnslett and Rausand (1999) define resilience as "*the ability to return to a stable situation after an accidental event*", assuming that it then can function at a sufficient level of capacity. Resilience is treated as opposite to vulnerability, which are the properties of a system that weakens or limits its ability to endure disruption. Further, resilience is different from robustness, as a robust system will resist accidental events, and remain at its initial stable situation. Accordingly, a resilient system is one which has the ability to adapt to the disruption, its performance recovered to a new stable situation (Asbjørnslett and Rausand 1999). Resilience becomes interesting in the context of vulnerability assessment, which compared to risk assessment puts a stronger emphasis on allocation of resources in response to accidental events.

In their report on resilience engineering, Dekker et al. (2008) define resilient systems as being "*able to effectively adjust its functioning prior to, during, or following changes and disturbances, so that it can continue to perform as required after a disruption, or a major mishap, and in the presence of continuous stresses*". While a basic description of resilience is often related the ability to bounce back, the definition given by Dekker et al. (2008) fits well with the proposition that resilient systems should both avoid, withstand, adapt to, and recover from disruption (Madni and Jackson 2009; Jackson and Ferris 2013). Chalupnik et al. (2013) place resilience within a framework of multiple "-ilities" for handling uncertainty in systems design. They define resilience as "*the ability of a system, as built/designed, to do its basic job or jobs not originally included in the definition of the system's requirements in uncertain or changing environments*". Chalupnik et al. (2013) contrast resilience with flexibility, as flexibility implies an active restructuring of system form, whereas resilience does not. Youn et al. (2011) see a resilient system as a reliable system that can be restored by finding alternative ways of functioning after perturbations.

Castet and Saleh (2012) define resilience as a superset of survivability and recoverability. Survivability is seen as a measure of the loss of performance due to the disruption. Hence, survivability relates to what often is considered avoidance and absorption of the effects of a disturbance. Recoverability is the time it takes to recover from the disruption, and represents the dynamic resilience that recovers the system after disruption. On the other hand, Richards (2009) sees resilience enhancement as one of several strategies for improving survivability. This perspective is particularily useful for defense systems. In this case, survivability becomes the leading attribute, while being supported by resilience. Richards (2009) defines resilience as "*the ability of a system to recover from disturbance-induced value losses within a permitted recovery time*".

In supply chain management, resilience is defined as "*the ability of a system to return to its original (or desired) state after being disrupted*" (Peck et al. 2003), or as "*the ability to bounce back from a disruption*" (Rice Jr. and Caniato 2003; Sheffi and Rice Jr. 2005). Resilience is also defined as "*the ability of the supply chain to handle a disruption without significant impact on the ability to serve the customer"* (Berle et al. 2011). Rice Jr. and Caniato (2003) suggests that flexibility and redundancy are primary strategies for building resilience into supply chains. Redundancy in the supply chain implies costs, while providing the flexibility to reroute should it be necessary. For example, a firm that sources from a second supplier may be spending more resources than absolutely necessary, indicating a redundancy. Still, the firm may be better off than its competitor with only one supplier should a disruption occur, as the firm now has the flexibility to switch from the primary to the secondary supplier.

In this paper, resilience is sought by exploiting latent functional capabilities to adapt to, and bounce back from system-internal disruptions, ie. failure modes. Failure modes are defined as loss of critical functionality in the system (Rausand and Høyland 2004). The focus on latent capabilities leads us to consider identification of alternative ways of functioning as the primary enabler of resilience. Hence, we limit the scope to studying reconfiguration of the function-form mapping of a designed system, rather than addressing reconfiguration of the form of the designed system. Still, more detailed design studies may reveal that this will imply re-wiring of certain links between system components.

2.2. Measuring resilience

Similar to the lack of agreement on qualitative definitions of resilience, there is a corresponding lack of agreement on formally defined, quantitative resilience metrics (Henry and Ramirez-Marquez 2012; Hosseini et al. 2016). Hosseini et al. (2016) classify quantitative models of resilience either as general resilience measures, or as structural measures. Structural measures use simulation and optimization models to understand the impact of design characteristics on resilience. General measures compare performance before and after disruption, and can be further separated into static and dynamic models.

Complex systems theory provide insight into the properties that ensure continued functioning through disruptions. Cohen et al. (2000) find that when node connectivity in complex systems follow a power law distribution they can continue to function even if a large number of nodes break down at random. As a small number of nodes carry most of the flow through the network, the probability that the network will break due to random disruptions is very low. However, Albert et al. (2004) find that these networks are extremely vulnerable to targeted attacks, as disruption of these highly connected "hubs" will be critical. Braha and Bar-Yam (2004, 2007) show that engineering problem-solving networks have comparable statistical properties. They argue that system structures are similar, making engineering systems vulnerable to poorly understood coupling between system components.

We now examine quantitative resilience metrics for practical decision support, with an emphasis on change in performance between two stable states, and the duration of disruption. Bruneau et al. (2003) use a resilience metric that assumes an instantaneous failure and a linear recovery profile, which considers the time it takes to fully restore the system performance. On this basis, Zobel (2011) develops a resilience function which accounts for decision-maker preferences with respect to the trade-off between the loss of performance due to the disruption and the disruption time. As these approaches assume a full recovery, they do not capture situations in which we can accept some permanent performance degradation, even though this could also provide a measure of how resilient a system is. Many other resilience metrics accept deviation between the system performance before disruption, and after recovery (Hosseini et al. 2016). This is consistent with acceptance of some permanent performance degradation, as seen from Fig. 1. Examples are Farid (2015), who presents a measure of actual resilience defined as the ratio between absolute performance before disruption and after recovery, Henry and Ramirez-Marquez (2012) who quantify system resilience as a function of time, and develop expressions for the total time and cost of bouncing back from disruption, and Francis and Bekera (2014) who measure resilience from the speed of recovery, and the performance level through the disruption and recovery process.

Resilience metrics relate to the system performance through a disruption, as shown in Fig. 1. Variations on this figure are found in a large number of publications on resilience (Asbjørnslett and Rausand 1999; Bruneau et al. 2003; Richards 2009; Henry and Ramirez-Marquez 2012; Ayyub 2014).

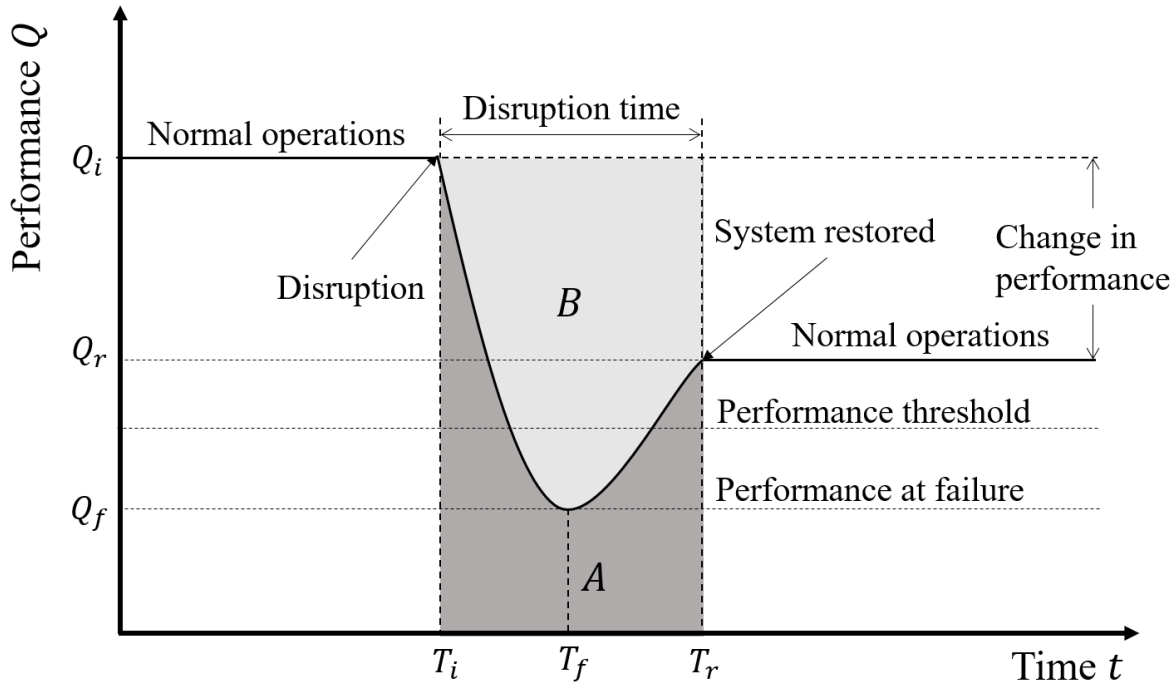


Fig. 1 Performance through a disruption, based on Asbjørnslett and Rausand (1999)

In Fig. 1, we observe a system initially operating at a performance level Q_i. A disruptive event is initiated at time T_i. The disruption is completely manifest at the time T_f, which is associated with a level of performance Q_f. Any performance below the performance threshold will imply system failure. At a time T_r, the system is recovered to an acceptable level of performance given by Q_r.

One of the most comprehensive resilience metrics studied is presented by Ayyub (2014). Ayyub (2014) defines system resilience R_e as given in Equation (1). In the formula, $\Delta T_f = T_f - T_i$, and $\Delta T_r = T_r - T_f$, following the notation from Fig. 1. The failure profile F depends on the type of failure event, and can be seen as a measure of the robustness and redundancy of the engineering system. The recovery profile R is a measure of the quality of actions we resort to during the recovery process. The resilience measure in Equation (1) is arguably difficult to apply in a practical decision-making context. Due to this concern, Ayyub (2015) reverts to a simplified resilience metric. The simplified resilience metric is presented in Equation (2). Here, T_e refers to the end of the planning horizon.

$$R_e = \frac{T_i + F\Delta T_f + R\Delta T_r}{T_i + \Delta T_f + \Delta T_r} \tag{1}$$

$$R_e = 1 - \frac{(T_r - T_i)(Q_i - Q_f)}{2Q_i T_e} \tag{2}$$

Compared to Equation (1), Equation (2) makes a few simplifying assumptions. First, it assumes a completely brittle failure, meaning that the failure materializes completely at the time of the disruption. Second, it assumes a full recovery to the initial level of performance. Third, the resilience will depend on the length of a notional planning horizon, indicating that resilience should also encompass the long term performance after full recovery. Hence, the resilience becomes dependent on the planning horizon. By increasing the planning horizon, the same system would receive a higher resilience measure than if a shorter planning horizon is used. For systems operating a process without a well-defined planning horizon, this measure may be especially misleading, as the planning horizon can be arbitrarily set to artificially increase resilience. If a system operates on a mission that is limited in time, this measure could work better, as the start and end times are given.

With reference to Fig. 1, another metric that captures resilience is presented in Equation (3). This resilience metric includes both the impact of the performance change and the disruption time on resilience. Here, the area A represents the performance through a disruption, and the area $A + B$ represents the undisrupted system performance in Fig. 1. This metric only captures the transient phases between the phases of normal operations.

$$R_e = \frac{A}{A + B} \tag{3}$$

Rather than concluding what is a right operationalization of resilience, it can be observed that resilience metrics include parameters related to performance, time, and cost. Fig. 2 shows that a more resilient system is one that ideally is able to effectively minimize the change in performance through a disruption ΔQ_r, minimize the disruption time ΔT_r, and minimize the cost of recovery C_R. Minimization of ΔT will likely be accomplished by minimizing ΔT_r, as this is the part of ΔT we can control.

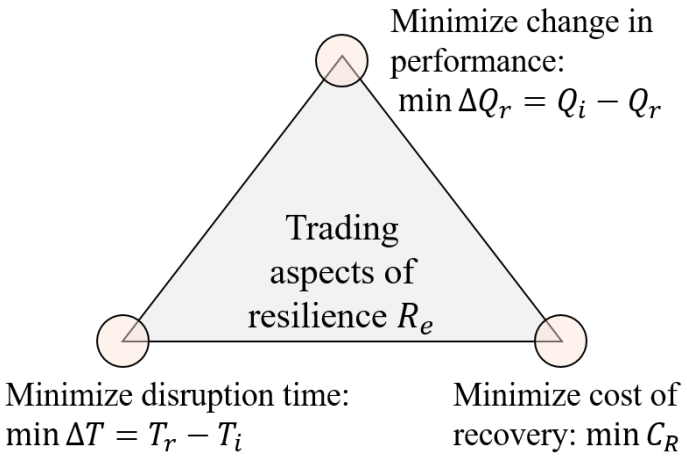


Fig. 2 *Trading three dimensions of resilience; change in performance, disruption time, and cost of recovery*

There are trade-offs between minimizing ΔQ_r, ΔT, and C_R. If system stakeholders prefer a swift reparation of a failed system to minimize delay of operations, this could compromise restoration of performance. Similarly, choosing a cheaper recovery solution is associated with a lower level of performance. Decision-makers should be encouraged to select a model of resilience most suited their preferences and scope of analysis, and to perform cost-benefit analyses or tradespace studies to evaluate alternative strategies for creating resilience (Madni and Jackson 2009).

We can hence quantify resilience by considering performance at time t, Q_t, as dependent on the current mapping between function and form. At time t, the functional requirements $\{\boldsymbol{FR}\}_t$ are met by a set of design parameters $\{\boldsymbol{DP}\}_t$. The functional and physical domains are linked via a design matrix $[\boldsymbol{A}]_t$, in accordance with axiomatic design (Suh 1990). Equation (4) relates the performance to the design parameters via the function-form mapping, as it changes over time, making the resilience profile dependent on the failure mode.

$$Q_t = f(\{\boldsymbol{FR}\}_t) = f([\boldsymbol{A}]_t \cdot \{\boldsymbol{DP}\}_t) \tag{4}$$

3. Latent functional capabilities

3.1. Manifest and latent functions

Merton (1968) first introduced the distinction between manifest functions, latent functions and dysfunctions to functional analysis in social science. The motivation for such functional analysis was to understand the unintentional consequences of policy. Policies have unforeseen effects, and there is a risk that a policy may have negative consequences outweighting the intended benefits. On the other hand, some unintended consequences are positive,

meaning that there is also a chance that the total outcome of the policy may be better than expected. Table 1 outlines this functional taxonomy in terms of the benefit, intent and recognition associated with the function.

Table 1 *Classifying functions according to benefit, intent and recognition*

Function	Positive	Intended	Recognized
Manifest	Yes	Yes	Yes
Latent	Yes	No	No
Dysfunctional	No	No	No

Manifest functions serves the purpose for which the system was originally designed, and can thereby be characterised as positive in the sense that they contribute to performance. Merton (1968) describe the manifest functions as represented as the cases when the "*subjective aim-in-view coincides with the objective consequence*". Dysfunctions are unintended, negative consequences, and will not be covered further in this paper. Latent functions are defined as the functions of an artifact that are "*neither intended nor recognized*" (Merton 1968), and can be a source of value by providing additional capabilities. A car is an example of an artifact whose functions not only includes the manifest transportation function, as cars regularly serve latent purposes. Some cars serve an aesthetic function and signal prestige, while other cars function as dwelling places for the homeless and travellers, or as barriers during rioting (Crilly 2010).

Even though most systems are designed based on the assumption that the correct function-form mapping is used, latent functional capabilities may arise due to inherent deviation between the intended, and the actual capabilities of a system. This is especially true for complex systems with emergent behaviour, for which it is hard to predict performance accurately. Indeed, some residual capabilities may exist due to deviations between the observed and the predicted system behaviour. This argument is in correspondence with Park et al. (2013), who state that resilience requires a new way of design thinking in which complex systems are never considered completely finished. While some actual capabilities beyond the intended capabilities could be revealed through system evaluation or once the system is fielded, some actual capabilities remain hidden. We should point out that while we propose that latent capabilities should become obvious to the system owner, they do not need to become so to the designer. In Fig. 3, the actual capabilities of an engineering system are divided according to the degree to which these match the intended capabilities, and to the degree that the related functions are desirable.

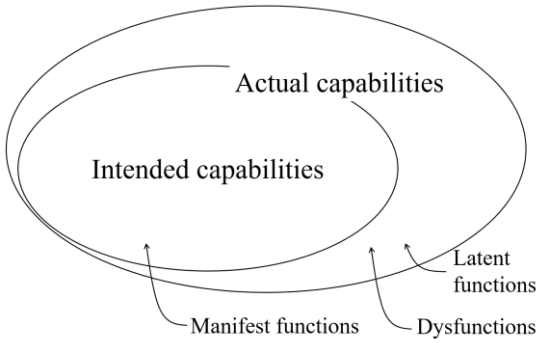


Fig. 3 *Mapping the functional taxonomy onto actual, and intended capabilities*

Following Fig. 3, latent functional capabilities do not result from the concious design process, but result from characteristics in designed artifacts that the designer did not specifically design for. These capabilities are positive functional byproducts of the designed form, which were outside the realm of perception during the design process, diverging from the intended function-form mapping. Instead, latent capabilities are uncovered through an additional analysis of the finished description of the design, after the closure of the design process, as the designers were unaware of these capabilities. Hence, the physical system form does not change when uncovering these capabilities. Latent capabilities will therefore likely have a lower cost compared to designing intentional redundancies, as it is only a question of activating capabilities already embedded in the system (Ross and Rhodes 2008).

Fig. 4 distinguishes between manifest and latent functional capabilities in the function-form mapping of a design. Here, the design parameter, DP_2, has latent functional capabilities that enable it to perform a functional requirement, FR_1, in addition to performing its manifest functional requirement, FR_2.

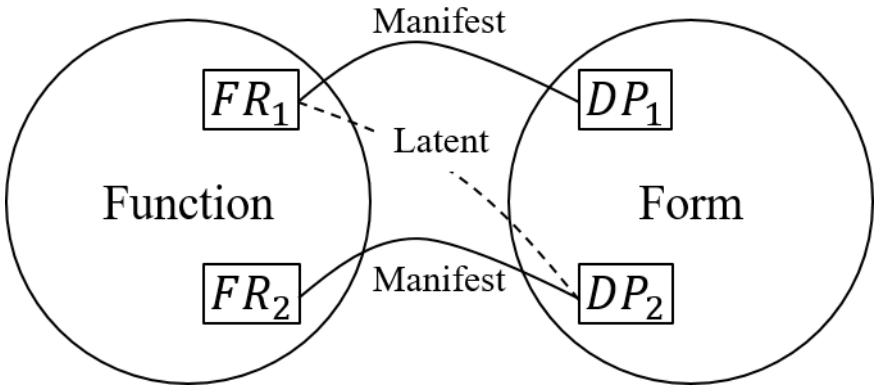


Fig. 4 *Separating manifest and latent functional capabilities in function-form mapping*

A manifest design with a desirable one-to-one mapping between function and form is presented in Equation (5). The design adheres with both the Independence Axiom and the Information Axiom (Suh 1990) at the closure of the design process. To indicate that this design performs at a stable level initially, the functional requirements are subscripted by T_i. The latent functions of any of the design parameters would be indicated by non-zero elements outside of the diagonal of the design matrix $\boldsymbol{A}$.

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix}_{T_i} = \begin{bmatrix} a_{11} & 0 \\ 0 & a_{22} \end{bmatrix} \begin{Bmatrix} DP_1 \\ DP_2 \end{Bmatrix} \tag{5}$$

Latent capabilities may seem like a logical contradiction. Our response to this likely objection to the concept, is that identification and recovery planning using latent capabilities is not to be viewed as a part of the design process itself, but is undertaken after the closure of the design process. Creating awareness of the existence of latent functions and their uses in the operational phase of a system, does not imply that we immediately make them active. The designers of the system do not even have to be consulted to identify latent capabilities, as the system owner can perform this assessment even after the system has been fielded. Further, system owners and users recognize system capabilities differently than the capabilities the designers.

3.2. Latent functional capabilities for resilience enhancement

During operation, the system described in Equation (5) will be subjected to disruptions caused by system-internal failure modes. Consider an event where a piece of equipment loses part of its manifest functionality, experiencing a failure mode (Rausand and Høyland 2004). The failure mode would constitute a disruption if the performance drops below the performance threshold presented in Fig. 1. We introduce a failure mode f into the manifest, uncoupled design in Equation (6) at a time T_f. Note that the failure mode only requires that we understand what functionality is lost, without requiring that we understand the exact scenario leading up to the failure (Berle et al. 2011).

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix}_{T_f} = \begin{bmatrix} a_{11} - f & 0 \\ 0 & a_{22} \end{bmatrix} \begin{Bmatrix} DP_1 \\ DP_2 \end{Bmatrix} \tag{6}$$

Assuming that the performance drops below the threshold for acceptable performance due to the failure, the system will need to bounce back to an acceptable performance level. To achieve this, there will be a need for adaptation of the function-form mapping to once again fulfill each FR in a sufficient manner. If there are latent functional capabilities in the other DPs of the system, we can reveal and reassign these to cover the lost functionality, leading to a recovery

of performance. Using the notation above, this would mean that there exists latently some design matrix element $a_{12} \neq 0$, which we introduce to provide the recovery r. We must now take into account a reduction c in the ability of DP_2 to fulfill FR_2, due to the current functional coupling. The corresponding function-form mapping after DP_2 has been repurposed to use its latent capability is shown in Equation (7).

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix}_{T_r} = \begin{bmatrix} a_{11} - f & r \\ 0 & a_{22} - c \end{bmatrix} \begin{Bmatrix} DP_1 \\ DP_2 \end{Bmatrix} \tag{7}$$

These design matrices can be used for evaluating the resilience of a system design when taking advantage of latent functional capabilities. Plugging Equations (5) – (7) into Equation (4), we can evaluate performance at interesting time steps, if we assume that we know the relationship between FRs and performance. The resulting expressions for performance as a function of time are entered into a resilience metric (Equation (1) – Equation (3)), allowing comparison with alternative strategies for resilience enhancement. In this section, we only suggest how this can be done in a generic manner, independent of the system performance metrics, and resilience metrics chosen.

In Fig. 5, the function-form mapping of the system is illustrated at two points in time, representing the system before failure, at time T_i (State A), and after recovery, at time T_r (State B). We consider the design to exist in two distinct system states, depending on the function-form mapping. Before failure, the system is operational as intended by the designers. The failure causes a complete loss of the ability of DP_1 to perform FR_1, indicated by $f = a_{11}$. After the recovery, the system again becomes operational by utilizing the latent functional capabilities provided by DP_2, as indicated by $a_{12} = r$.

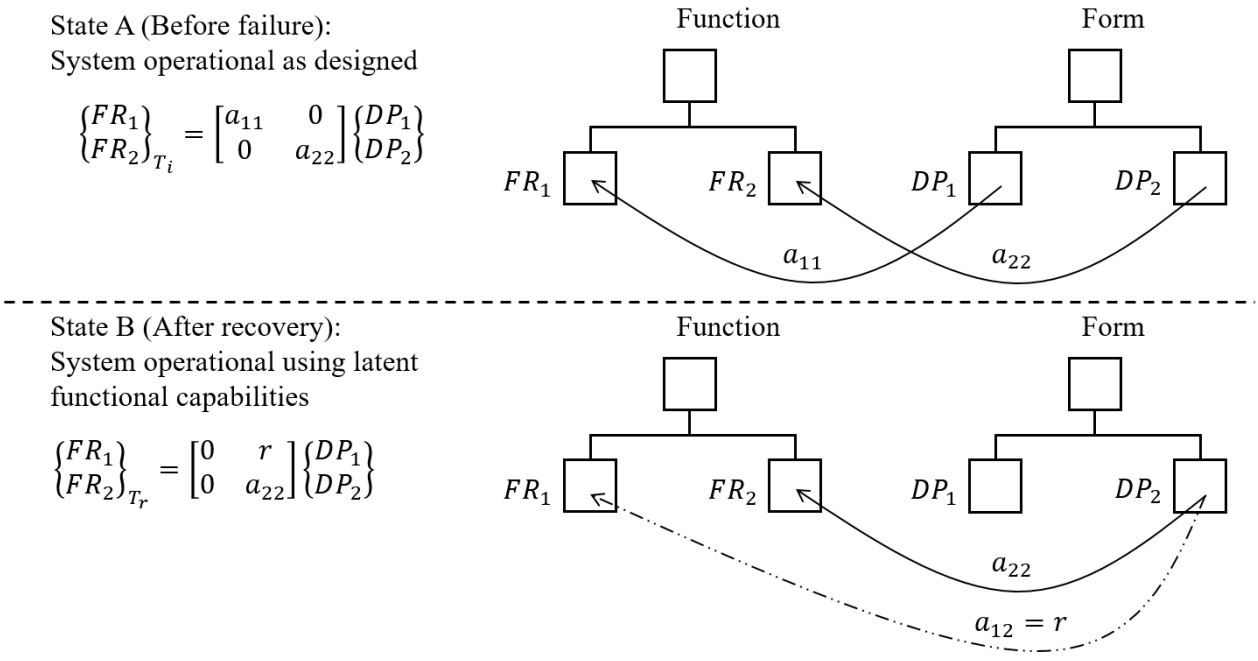


Fig. 5 *Function-form mapping before disruption, and after a complete recovery using latent functional capabilities*

3.3. Implications for the design axioms

We here discuss the implications of latent functional capabilities on the design axioms. The independence axiom states that we want to keep functional requirements independent from each other (Suh 1990), preferably by designing uncoupled systems, with a one-to-one mapping between functional requirements and design parameters, as seen in Equation (5). While the function-form mapping proposed in Equation (7) is seen as an improvement from the failed system state described by Equation (6), it is nevertheless a decoupled design rather than an uncoupled design, indicating a less desirable system state. A functionally coupled design breaks with the Independence Axiom, meaning that the

system should be repaired, or redesigned. As the resources of a system's DPs are limited, functional coupling will impact the fulfillment of the other FRs.

The information axiom states that the information content of a design should be minimized, as a large information content reduces the probability of meeting the FRs (Suh 1990). Braha and Maimon (1998) makes the distinction between the structural and functional complexity of a design. They argue that the structural complexity of a system can be quantified from the information needed to declare the system form (DPs), as a function of the number of parts and interfaces. They define the functional complexity in adherence with the information axiom, so that a system that maximizes the probability of meeting all functional requirements, is the best physical solution. Considering latent capabilities will not impact the structural complexity of the system under consideration in Equations (5) – (7). The uncoupled design in Equation (5) is transformed through disruption and recovery to the coupled design described by Equation (7). In Equation (7), the system is in a state where the FRs are coupled. This reduces the probability of meeting the FRs, which implies an increase in functional complexity.

An example of a likely problem is task scheduling when using latent capabilities, as one DP will be unable to perform two functions simultaneously. If an operation consists of two tasks that are required to be performed simultaneously, but are not co-located, relying on latent capabilities may not work at all, as an artifact can only be in a single place at a time. Due to the functional coupling, the function-form mapping based on latent functional capability should not be considered an end state for the system. Rather, the use of latent functional capabilities should be seen as a temporary means to avoid severe consequences of a prolonged disruption of operations, or as a means to safely shut down operations.

The overall implications of using latent capabilities to recover from disruption, are partially counter to the design axioms. We see that functional coupling creates an opportunity to recover from an adverse condition of reduced overall functionality. The coupling thereby contributes to enhancement of resilience, at the expense of an increase in functional complexity, which makes the system overall less likely to meet all its FRs. However, the alternative to not taking advantage of the latent capabilities and accept functional coupling, is to remain inoperable. Facing this alternative, the pragmatic approach is to accept deviation from the design axioms in order to attempt to regain operability via latent capabilities, given that increased risk of further failure due to the coupling are accepted.

4. Including latent capabilities in engineering systems

We have seen how system resilience can be enhanced by efficiently exploiting latent functional capabilities, which the designers did not intend nor recognize before fielding the system. For exploitation of latent capabilities to become a viable strategy for increasing resilience, we need a structured approach to identify latent capabilities and plan for their use. We propose two steps that should follow after the closure of the design process:

1. Search for latent functional capabilities to enhance resilience in case of disruptions.
2. Plan recovery from disruption using latent functional capabilities.

4.1. Search for latent capabilities

We propose that an additional search for latent capabilities can be performed on the basis of the output of the design process. At closure of the design process, the output is a description of the physical form that will perform a set of functional requirements, derived through some synthesis. At this point, the design will adhere to some mapping between FRs and DPs, as shown in Section 3.

Searching for latent capabilities, we seek to identify alternative ways the same needs can be satisfied by the described physical system. Table 2 proposes methods that support the search effort that can be undertaken with the purpose of uncovering latent capabilities. The taxonomy in Table 2 classifies methods according to the level of abstraction required to apply them in the search for latent capabilities, making a distinction between discovery of latent capabilities through function-based, and value-based search for latent capabilities. Value-based search will here refer to methods that move from meeting the functional requirements that were disrupted, towards meeting the higher level functions, and ultimately needs that the functional requirements support.

Table 2 *Search methods for latent functional capabilities*

Level of abstraction	Examples of useful concepts and methods for identification of latent capabilities
Function-based	Model testing (prototypes, CAD models)
	Learning from similar designs in operation
	Failure modes
	Design catalogues
Value-based	Goal abstraction
	Framing of decisions

4.1.1. Function-based identification

Function-based methods for identification seek to identify latent functions in system components, that may be used to replace lost manifest functionality in other system components. We consider the design process to close with a description of the system to be built. This description can include drawings, various models, prototypes, and user manuals. System descriptions can be analyzed to provide insights into possible functioning that was not planned for in the design process, finding latent capabilities. For example, can a component whose purpose is to perform a specific function, perform a function currently performed by a different component in the system? In relation to the design process, function-based identification of latent capabilities is a process of analysis, rather than synthesis, mapping from form to function, after the closure of the design process (which primarily maps from function to form).

To test whether finished design descriptions possess useful latent capabilities, we evaluate its performance against possible failure modes. For example, a simulation setup can be devised where system components are deliberately removed, to see if the system reorganizes in such a way that another component steps in to cover the lost functionality. We can then study the overall effects on post-removal system performance. In such a simulation setup, we could implement decision rules that would suggest which components to assign to cover lost functionality. Alternatively, human system operators could be challenged to find work-around solutions to recover from the disruption.

Existing tools for system analysis could provide insight in this function-based identification procedure for latent capabilities. Failure Modes, Effects, and Criticality Analysis (FMECA) comes from reliability engineering, and is used for identification and criticality assessment for failure modes (Rausand and Høyland 2004). Berle et al. (2011) study failure modes in maritime transportation systems, and argue that it is possible to understand which functionality is most critical without understanding the scenario leading up to the failure. This insight is useful when directing the search for latent capabilities. By identifying the functions whose loss would have the largest consequences, we can aim the search for latent capabilities on recovering these functions. An FMECA may already have been done to support decisions regarding manifest redundancies in the design process, often on the basis of criticality as a product of probability and consequence. In contrast, here we assume that we only need to quantify how a failure mode will affect performance, as we are interested in whether it is possible to recover functionality.

Tools from the design process can also provide support for discovering latent capabilities to cover the failure modes. Design catalogues are one example. A design catalogue provides collections of proven solutions to design problems, at differing levels of embodiment or fidelity, and represents a comprehensive look-up table for finding solutions to problems quickly (Pahl and Beitz 1996). A design catalogue could for example provide an overview of solution concepts (forms) mapped onto the functions to be achieved by the designed system. Design catalogue can be used to identify latent capabilities in the following manner: Assume that the design process closes and we possess a description of the system meeting a set of functional requirements. In this system description, Function 1 is met by Subsystem 1, and Function 2 is met by Subsystem 2. However, the design catalogue reveals that it is possible to achieve Function 1 using Subsystem 2, without this being intended by the designers. Hence, we can conclude that Function 1 is a latent function for Subsystem 2. This provides the system as a whole with the latent capabilities to recover from a failure mode in Subsystem 2, if this reorganization is feasible.

4.1.2. Value-based identification

Abstraction from functional requirements to objectives can cast additional light on the problem of identifying latent capabilities. Perhaps the designers and operators of the disrupted system should have realized that the loss of functionality is critical only as long as the fulfillment of the stated functional requirements in a narrow sense is what defines success. Like the mapping from function to form, the set of functional requirements meeting the stated needs is likely non-unique. Suh (1990) includes the mapping from customer needs to functional requirements in the axiomatic design approach. Hence, the formation of functional requirements can also be seen as an open-ended design process, much like the formation of design parameters on basis of functional requirements. An abstraction to the level of values, goals and objectives hence opens the solution space, and helps us uncover a larger number of latent capabilities than otherwise possible. Value-based identification of latent capabilities could be obtained by redefining the cognitive frames with which we view the problem of recovering from disruption. Framing a design problem in a slightly altered manner can then make certain aspects of the problem at hand obvious, as this would alter the designer conceptions of the purpose of the system (Tversky and Kahneman 1981). A relevant framework that can be consulted for the purpose of identifying latent capabilities on the basis of value, is presented by Ross and Rhodes (2008). They suggest a classification scheme that ranks favorable system attributes according to the degree to which these attributes were articulated as needs by the stakeholders, and the extent to which these needs can be met through the system lifecycle without incurring large costs.

As an example of how value-based identification of latent capabilities could work, we can consider the case of a marine transportation system supplying crude oil. This system could fail to fulfill its function, for example due to a blocked port terminal. A solution to the problem does not need to lie in the functional space, where we find existing capabilities that can restore the terminal function. Instead of seeking to recover the function “supply oil to community”, we can abstract to the overall objective, which is to “provide energy to the community”. With this abstraction, many more solutions can be found to latently meet the objective, and resolve the current situation.

4.2. Planning recovery using latent capabilities

The search process for latent capabilities may provide us with a set of strategies to enhance resilience. Before deciding on use of latent capabilities, the effectiveness of this should be compared to adding redundancy or recovery systems after closure of the design process. Against certain failure modes, redesigning to include redundancies may be better than using latent capabilities. Typical cases where other recovery strategies may be more effective, include situations where the capacity of a system component to perform its intended function is greatly reduced by functional coupling, or situations where latent capabilities introduce new risks. Selection of recovery strategy depends on stakeholder dependent performance, and resilience metrics. System stakeholders have different preferences towards the trade-off between change in performance through the disruption (ΔQ), disruption time (ΔT), and the cost of recovery (C_R). Stakeholder A may care a lot about a swift recovery to an acceptable performance level, whereas Stakeholder B may prefer a slower recovery and have higher expectations regarding the performance level after the disruption.

There are many potential constraints that may limit the applicability of latent capabilities for resilience enhancement. Even if we assume technical feasibility, regulatory concerns and the organizational aptitude towards planning for recovery using latent capabilities need to be considered. As an example of regulatory constraints, we can consider rule-based standards that act as the backbone of safety regulations in ship design (Papanikolaou 2009). Under this regulatory regime, ship designers follow rules that regulate the form of ships. While rule-based regulations could limit the degree to which one can plan to use latent capabilities for resilience enhancement, current trends indicate a move towards goal-based regulations. The move to goal-based standards in ship design is believed to open the solution space, as it allows designers to proactively consider different solutions. Exploiting latent capabilities may be analogous, as this opens new opportunities for functioning, as long as it can be shown that using latent capabilities will provide outcomes that are at least as resilient. In any case, deviations from normal operating patterns will often require detailed analysis to show that using latent capabilities do not increase the vulnerability of the system towards other threats.

The organizational aptitude towards using latent capabilities in the engineering system for increasing resilience is another constraint. Sutcliffe and Vogus (2003) point to organizational processes aimed at enhancing overall competence and growth, and the ability to rearrange resources to deal with new situations as two primary enablers of resilience. Organizations vary in their ability to learn from previous experience, and their ability to use these lessons

to adapt efficiently to new operating conditions and alter function-form mapping to recover performance. Constraints to using latent capabilities may exist on several levels in the organizational hierarchy. System managers differ in their willingness to investigate latent capabilities as a recovery strategy, and with respect to whether they will prioritize making latent capabilities part of contingency plans to address disruptions. System operators differ with respect to previous experience with disruptive events, rendering some operators particularly well-suited to ensure that the engineering system adapts to disruption, restoring operations by taking advantage of latent capabilities.

Recovery planning via latent capabilities can be summarized as follows: First, we need to evaluate whether latent capabilities is the favored way to address each failure mode. Note that this does not require us to identify how a function fails, but only what to do when it fails. Second, if a failure mode should be addressed via latent capabilities, we should develop operational procedures that define how human system operators should act to facilitate the reordering of function-form mapping, so that functionality is restored. Third, the organization managing the engineering system needs to ensure sufficient knowledge sharing and training to support fulfillment of these procedures.

5. Illustrative cases

5.1. AHTS vessel operational recovery

Anchor handling, tug, supply (AHTS) vessels perform functions such as lifting of anchors, towing of offshore rigs, and supplying oil platforms (Erikstad and Levander 2012). These vessels are normally outfitted with powerful winches for towing and anchor handling. The vessels are also increasingly employed in certain subsea operations, for example using cranes to lift and deploy remotely operated vehicles (ROVs).

We consider an offshore operation where an ROV is deployed from an AHTS vessel. The ROV is launched and recovered using a crane installed on the vessel. An event occurs where the crane experiences a failure mode, losing some or all of its manifest lifting capability during the ROV operation. As the ROV is deployed using the crane which has lost its lifting capacity, it is now impossible to retrieve the ROV using the crane. To recover the ROV, we propose that the winch also installed on the vessel, latently possesses the ability to perform the lifting function, enabling it to retrieve the ROV. The physical effects needed to perform the towing function in the horizontal direction, are similar to the physical effects needed to provide the lifting function in the vertical direction. The latent lifting function of the winch would be identified by studying a design catalogue with overview of alternative solution principles for the lifting function.

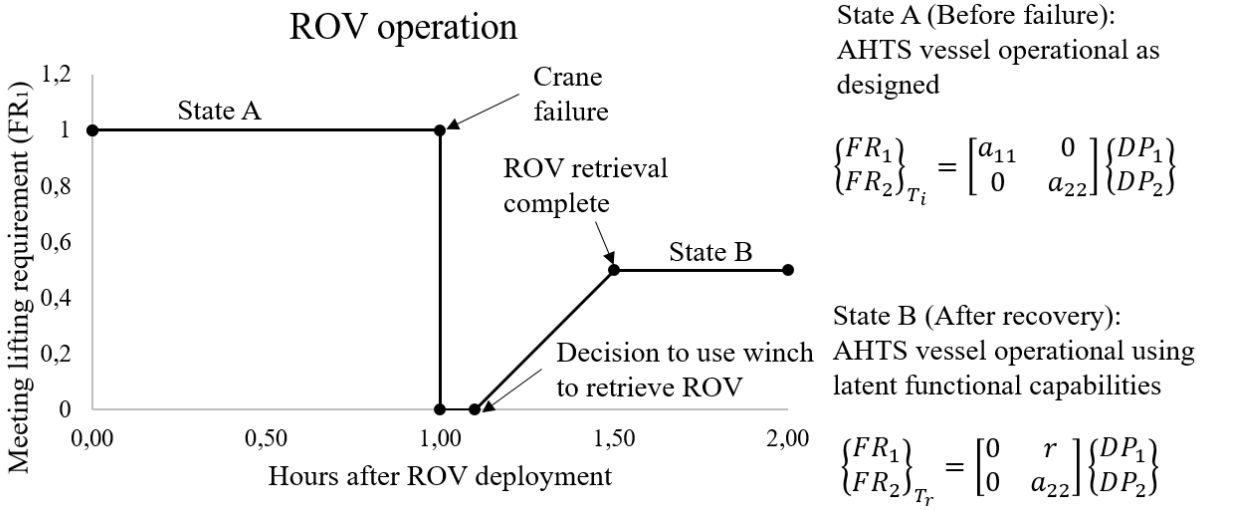


Fig. 6 The relationship between resilience and latent capabilities for the AHTS crane failure event. To the left, we see the performance profile initially (State A), through the crane failure and recovery (State B). To the right, we see the function-form mapping equations describing the system in State A and State B. State A describes the system before disruption, and State B describes the system after recovery.

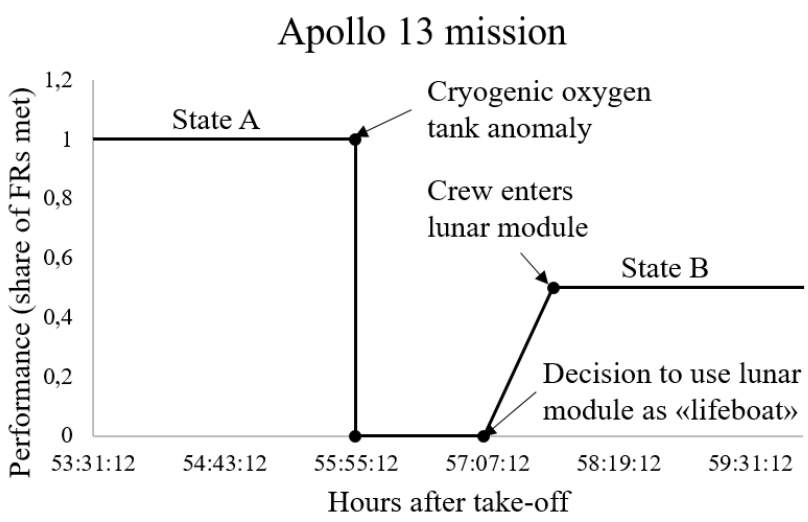
Fig. 6 illustrates the performance profile of the AHTS vessel systems over the duration of the operation and crane failure. Performance in Fig. 6 is measured by the ability of the vessel to meet FR_1, which is to perform the lifting function. FR_2 represents the towing function, and meeting this FR does not impact performance during the ROV operation. DP_1 refers to the crane onboard, while DP_2 refers to the winch onboard. In State A, the system operates as planned, as an uncoupled design. We assume that the elements of the design matrix $a_{11} = a_{22} = 1$, to signify that FRs are exactly met by the DPs. Once the crane fails, a_{11} goes to 0. As we find that the winch can be used to lift the ROV, the function-form mapping is rearranged. This is referred to as State B, in which the design matrix contains the element r. The performance profile accounts for the differences in how well the crane and winch perform the lifting function, by considering the quality of the lifting function as 50% of the quality associated with the manifest lifting functionality, meaning that $r = 0.5$. This reduction in functional quality can relate to crew competence with operating the winch in a new way, or the risk of damages due to impact between the ROV and the vessel stern when pulling the ROV up into the vessel using the winch. These are examples of limitations that should be investigated as part of the process of planning how to use latent capabilities.

5.2. Apollo 13 spacecraft recovery

The Apollo 13 mission is remembered for the creative problem solving process after its planned mission to the Moon was aborted due to a series of critical system failures affecting the Command and Service Module (CSM). The overall mission statement for Apollo 13 can be described as transporting three crew members safely from the Earth to the Moon, and back. The manifest design of the Apollo 13 spacecraft can be described as an uncoupled system on a high level. The manifest function of the CSM was to transit through space supporting a crew of three men. On the other hand, the manifest function of the lunar module (LM) was to transport two crew members between the CSM in lunar orbit and the lunar surface, and back. Due to the loss of critical functions in the CSM, this normal operating procedure became impossible.

The mission review report (Cortright 1970) documents the accident and recovery effort. A fire in one of the oxygen tanks, initiated by an electrical short circuit, lead to loss of multiple oxygen tanks and several fuel cells. According to the accounts made by lead flight director Gene Kranz (Kranz 2000), nothing remotely close to this sequence of events had happened in mission simulation, showing characteristics typical for normal accidents (Perrow 1999). The seriousness of the situation quickly showed that the lunar landing would have to be aborted, the mission objective shifting to survival.

The response and recovery from the critical failure of the CM, to a state where return to Earth was possible, can be considered a successful process of identification and exploitation of latent functional capabilities found in the Lunar Module (LM) of the spacecraft. At the time of the failure, attention turned to calculating whether there was sufficient power and oxygen in the LM to support the three-person crew for the extended period required to return to Earth, equivalent to the identification phase described in Section 4. After concluding that this approach to operating the spacecraft was the most likely to ensure survival, the next step was to plan how the recovery would commence. In this next phase, the flight operators set to develop the procedures for the maneuvers to get home. Hence, the functions of the CSM were reassigned to the LM, which essentially took the role as “lifeboat” for the crew (Cortright 1970). Implementation of these plans required the combined efforts of ground control personnel and the crew in space, to find work-around solutions that enabled the LM to support lost functionality. Even though scenarios implying that the LM could be used for life support in some emergencies had been thought of, its use in the scenario that actually played out was unprecedented (Cass 2005), and the transit back to Earth was not without challenges. As the LM was designed to support a crew of two for a two-day expedition to the surface of the moon, rather than a crew of three for a four-day return trip to Earth, preservation of consumables became necessary. Non-essential systems were powered down to reduce the usage of water, oxygen and energy.



State A (Before failure): Spacecraft operational as designed

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix}_{T_i} = \begin{bmatrix} a_{11} & 0 \\ 0 & a_{22} \end{bmatrix} \begin{Bmatrix} DP_1 \\ DP_2 \end{Bmatrix}$$

State B (After recovery): Spacecraft operational using latent functional capabilities

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix}_{T_r} = \begin{bmatrix} 0 & r \\ 0 & 0 \end{bmatrix} \begin{Bmatrix} DP_1 \\ DP_2 \end{Bmatrix}$$

Fig. 7 The relationship between resilience and latent capabilities for the Apollo 13 mission. To the left, we see the performance profile initially (State A), through the CSM failure, and recovery using the LM (State B). To the right, we see the function-form mapping equations describing the system in State A and State B. State A describes the system before disruption, and State B describes the system after recovery.

Fig. 7 shows the performance profile resulting from operating the spacecraft through the accident. We consider performance to be given by the share of FRs that can be met, conditional on crew survival until return to Earth. The transit function is represented by FR_1, and the landing function is represented by FR_2. The CSM is represented by DP_1, and the LM is represented by DP_2. For simplicity, we assume that $a_{11} = a_{22} = 1$, indicating that during normal operations (State A) the system is in a condition where the DPs exactly meet the FRs. Then, the functionality of the CSM is completely lost due to the accident, meaning that a_{11} goes to 0. To recover from the accident, latent functionality in the LM is found and plans are implemented to alter the function-form mapping, so that the LM is completely repurposed to perform the transit function, signified by r in the design matrix. In State B, we consider $r = 1$, as the use of the LM was sufficient to ensure return and survival of the crew. In State B, $a_{22} = 0$ because the LM was now reassigned to the transit function, at the sacrifice of performing the landing function.

Learning from the Apollo 13 incident triggered investigations into developing the lifeboat capabilities of the LM for future Apollo missions (Cortright 1970). As design changes were introduced to accommodate the possible use of the LM as a lifeboat, capabilities that were latent to the stakeholders in Apollo 13 until recovery from the failure, became part of the manifest design as a secondary functional mode to be used in case of functional failure.

It should be noted that the Apollo 13 recovery is an example in which latent capabilities is used to provide a safe conclusion to a mission, rather than continued operations. To take advantage of the functional couplings, it was necessary to abort the lunar landing, as the remaining resources had to be spent on the effort to safely return to the Earth.

6. Discussion

Our position is that latent capabilities can enhance system resilience against disruption. We have shown that systems can provide latent functions that were neither intended nor recognized by the designers, but nevertheless can become useful. These latent functions are outside the perceived range of system uses at the closure of the design process. For this reason we suggest that additional steps for identifying and evaluating whether latent capabilities can cover failure modes. The idea that a system can possess latent capabilities not currently active, not intended by the designers, and not currently recognized, is in agreement with the idea that complex engineered systems are never truly finished as they exhibit emergent behaviour that lead to an increase in our understanding of their capabilities through the

operational phase. The adaptation of system function-form mapping that define latent capabilities clearly represent a way for resilient systems to bounce back from disruption.

A likely criticism of the terminology introduced by this paper, is that inclusion of latent capabilities in design may appear contradictory. The solution to this terminological problem is to view the method proposed in Section 4 as an additional assessment taking place after the closure of the design process. This is essentially an additional step of analysis rather than synthesis, where alternative ways of functioning are examined. This procedure does not need to involve the team of designers that produced the system description from its functional requirements. In fact, the procedure we propose can also be done for systems that already are in operation. This highlights the difference between the perspectives of the system designers and the system users. As Crilly (2010) points out, the functionality the system user perceives can differ from the functionality intended by the system designers.

The propositions of this paper are in partial opposition to axiomatic design theory. Axiomatic design promotes functional independence and minimization of complexity (Suh 1999). Latent capabilities are based on the existence of functional couplings that the designers were unaware of. When using latent capabilities to bounce back from a disruption, the system enters a mode of operation where it breaks with the design axioms. The resulting functional coupling increases the functional complexity of the system. Therefore, use of latent capabilities challenges the common notion that it is always favourable to reduce complexity. A compromise could be that the designers seek to reduce complexity, whereas after the system has been fielded we seek to understand how operators can take advantage of latent capabilities resulting from the inability of designers to remove all residual complexity. In settings where continuation of operation outweighs concerns for avoiding functional coupling and for meeting every functional requirement, system stakeholders should seek to exploit latent capabilities. After all, in many situations it is better to restore the system, and operate it in a more complicated manner, than not operating at all. This perspective hence limits the role of axiomatic design to providing structure to the design process.

To apply latent capabilities, we need to understand the limitations of this approach: 1) If latent capabilities do exist, how much does exploitation of latent capabilities impact the intended behaviors? For example, we saw from the two case studies that the use of latent capabilities increased the load on system components that did not fail. In the Apollo 13 case, this made it necessary to deviate from the original mission scope by returning to Earth without visiting the Moon. 2) Does exploitation of latent capabilities introduce new operational and safety risks? For example, it is possible that operating some types of equipment outside its intended scope of functionality leads to excessive loads on the equipment and other system components, that can cause another failure with potential to propagate to other parts of the system.

In response to the concerns above, a methodology that can be used to assess the effectiveness of latent capabilities as a mechanism for enhancing resilience is needed. Established tools like FMECA, and design catalogues direct and enable the search for latent capabilities in the engineering system, and abstraction from current solutions and lower-level functions to higher-level functions and objectives also provide a path to identification of latent capabilities. The latent capabilities found must also be evaluated against other means to increase resilience. Our review found that there is little agreement on a specific operationalization of resilience, even though all are based on three main dimensions; change in overall system performance, disruption time, and cost of recovery. Alternatives to use of latent capabilities for resilience enhancement should be tested against these dimensions. Upon making a decision regarding the strategy for resilience enhancement, potential constraints must be taken into account, like the emergence of new risks, the role of regulation, and the ability of the managing organization to reorder the function-form mapping of the engineering system. Effective use of latent capabilities for resilience enhancement will require planning, and an organization that is able to alter the system functioning once a disruption materializes (Sutcliffe and Vogus 2003). The characteristics of resilient organizations, and the role of management and human system operators within these organizations should be studied further, to understand what it actually takes to exploit latent capabilities to enhance resilience.

7. Conclusion

This paper introduces latent capabilities as the capabilities of systems not intentionally designed for. Our position is that latent functional capabilities provide the ability to enhance system resilience against failure modes that disrupt systems from their normal operation. This paper shows that latent capabilities allow the function-form mapping of a

system to be changed in response to disruption. Importantly, latent capabilities are outside the perceived system uses envisioned by the system designer through the design process. Identification and planning for use of latent capabilities take place after the closure of the design process.

Our findings constitute a challenge to axiomatic design theory, as we show that adhering to the design axioms while facing a disruption may be counter to latent capabilities that enhance resilience. Counter to the design axioms, we find that designs that become coupled once latent capabilities are exploited, are able to recover from disruption, even though this implies that the system is more complex than originally intended. Hence, there is a trade-off between system resilience achieved through latent capabilities, and minimization of complexity in engineering systems that requires further exploration.

To provide empirical support for the arguments put forth in this paper, future work should investigate design cases in more detail, in which complex engineering systems have bounced back from disruptions using latent capabilities. Learning from these cases would strengthen the applicability of this approach and set latent capabilities into the context of practical situations. Specific topics that should be addressed include the constraints to using latent capabilities for recovery. This includes investigation of organizational traits that enable successful alteration of function-form mapping, and feasibility of latent capabilities given alternative regulatory regimes.

References

Albert R, Jeong H, Barabasi A-L (2004) Error and attack tolerance of complex networks. Nature 406:378–382.

Asbjørnslett BE, Rausand M (1999) Assess the vulnerability of your production system. Prod Plan Control 10:219–229.

Ayyub BM (2014) Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making. Risk Anal 34:340–355.

Ayyub BM (2015) Practical Resilience Metrics for Planning, Design, and Decision Making. ASCE-ASME J Risk Uncertain Eng Syst Part A Civ Eng 1:1–11.

Berle Ø, Rice Jr. JB, Asbjørnslett BE (2011) Failure modes in the maritime transportation system: a functional approach to throughput vulnerability. Marit Policy Manag 38:605–632.

Braha D, Bar-Yam Y (2007) The Statistical Mechanics of Complex Product Development: Empirical and Analytical Results. Manage Sci 53:1127–1145.

Braha D, Bar-Yam Y (2004) Topology of large-scale engineering problem-solving networks. Phys Rev E 69:16113.

Braha D, Maimon O (1998) The measurement of a design structural and functional complexity. IEEE Trans Syst Man, Cybern - Part A Syst Humans 28:527–535.

Braha D, Reich Y (2003) Topological structures for modeling engineering design processes. Res Eng Des 14:185–199.

Bruneau M, Chang SE, Eguchi RT, et al (2003) A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthq Spectra 19:733–752.

Cass S (2005) Apollo 13, We Have a Solution. In: IEEE Spectr. http://spectrum.ieee.org/aerospace/space-flight/apollo-13-we-have-a-solution#. Accessed 13 Mar 2017

Castet JF, Saleh JH (2012) On the concept of survivability, with application to spacecraft and space-based networks. Reliab Eng Syst Saf 99:123–138.

Chalupnik MJ, Wynn DC, Clarkson PJ (2013) Comparison of Ilities for Protection Against Uncertainty in System Design. J Eng Des 24:814–829.

Cohen R, Erez K, Ben-Avraham D, Havlin S (2000) Resilience of the Internet to random breakdowns. Phys Rev Lett 85:4626–4628.

Cortright EM (1970) Report of Apollo 13 Review Board. Washington, D.C.

Crilly N (2010) The roles that artefacts play: Technical, social and aesthetic functions. Des Stud 31:311–344.

de Weck OL, Roos D, Magee CL (2011) Engineering Systems: Meeting Human Needs in a Complex Technological World. The MIT Press, Cambridge, MA

Dekker S, Hollnagel E, Woods D, Cook R (2008) Resilience Engineering: New directions for measuring and maintaining safety in complex systems. Lund, Sweden

Erikstad SO, Levander K (2012) System Based Design of Offshore Support Vessels. In: IMDC 2012.

Farid AM (2015) Static Resilience of Large Flexible Engineering Systems: Axiomatic Design Model and Measures. IEEE Syst J 1–11.

Francis R, Bekera B (2014) A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliab Eng Syst Saf 121:90–103.

Henry D, Ramirez-Marquez JE (2012) Generic metrics and quantitative approaches for system resilience as a function of time. Reliab Eng Syst Saf 99:114–122.
Holling CS (1973) Resilience and Stability of Ecological Systems. Annu Rev Ecol Syst 4:1–23.
Hosseini S, Barker K, Ramirez-Marquez JE (2016) A review of definitions and measures of system resilience. Reliab Eng Syst Saf 145:47–61.
Jackson S, Ferris TLJ (2013) Resilience Principles for Engineered Systems. Syst Eng 16:152–164.
Klinke A, Renn O (2002) A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based and Discourse-Based Strategies. Risk Anal 22:1071–1094.
Kolmogorov AN (1983) The Combinatorial Foundations of Information Theory and the Probability Calculus. Russ Math Surv 38:29–40.
Kranz G (2000) Failure is not an Option: Mission Control from Mercury to Apollo 13 and Beyond. Simon & Schuster, New York, NY
Liu C, Hildre HP, Zhang H, Rølvåg T (2015) Conceptual design of multi-modal products. Res Eng Des 26:219–234.
Lundberg J, Johansson BJE (2015) Systemic resilience model. Reliab Eng Syst Saf 141:22–32.
Madni AM, Jackson S (2009) Towards a Conceptual Framework for Resilience Engineering. IEEE Syst J 3:181–191.
Mekdeci B, Ross AM, Rhodes DH, Hastings DE (2015) Pliability and Viable Systems: Maintaining Value under Changing Conditions. IEEE Syst J 9:1173–1184.
Merton RK (1968) Social Theory and Social Structure. MacMillan Publishing Co., New York, NY
Newman MEJ (2005) Power laws, Pareto distributions and Zipf's law. Contemp Phys 46:323–351.
Pahl G, Beitz W (1996) Engineering Design, 2nd edn. Springer, London, UK
Papanikolaou AD (2009) Risk-Based Ship Design. Springer, Berlin, Germany
Park J, Seager TP, Rao PSC, et al (2013) Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Anal 33:356–367.
Peck H, Abley J, Christopher M, et al (2003) Creating Resilient Supply Chains: A Practical Guide. Cranfield, UK
Perrow C (1999) Normal Accidents: Living with High-Risk Technologies. Princeton University Press, Princeton, NJ
Rausand M, Høyland A (2004) System Reliability Theory: Models, Statistical Methods and Applications, 2nd edn. John Wiley & Sons, Inc., Hoboken, NJ
Rice Jr. JB, Caniato F (2003) Building a secure and resilient supply network. Supply Chain Manag Rev 7:22–30.
Richards MG (2009) Multi-Attribute Tradespace Exploration for Survivability. Massachusetts Institute of Technology
Ross AM, Rhodes DH (2008) Using Attribute Classes to Uncover Latent Value during Conceptual Systems Design. In: SysCon 2008 - IEEE International Systems Conference. Montreal, Canada,
Sheard S, Mostashari A (2008) A Framework for System Resilience Discussions. INCOSE Int Symp 18:1243–1257.
Sheffi Y, Rice Jr. JB (2005) A Supply Chain View of the Resilient Enterprise. MIT Sloan Manag Rev 47:41–48.
Stern A (2015) Testimony before the House of Representatives Committee on Science, Space, and Technology. Exploration of the Solar System: From Mercury to Pluto and Beyond. Washington, D.C.
Suh NP (1990) The Principles of Design. Oxford University Press, New York, NY
Suh NP (1999) A Theory of Complexity , Periodicity and the Design Axioms. Res Eng Des 11:116–132.
Sutcliffe KM, Vogus TJ (2003) Organizing for resilience. In: Cameron K, Dutton JE, Quinn RE (eds) Positive Organizational Scholarship: Foundations of a New Discipline. Berrett-Koehler, San Francisco, CA, pp 94–110
Tversky A, Kahneman D (1981) The framing of decisions and the psychology of choice. Science (80-) 211:453–458.
Wildavsky A (1988) Searching for Safety. Transaction Press, New Brunswick, NJ
Woods DD (2015) Four concepts for resilience and the implications for the future of resilience engineering. Reliab Eng Syst Saf 141:5–9.
Youn BD, Hu C, Wang P (2011) Resilience-Driven System Design of Complex Engineered Systems. J Mech Des 133:101011.
Zobel CW (2011) Representing perceived tradeoffs in defining disaster resilience. Decis Support Syst 50:394–403.