Comparison of ilities for protection against uncertainty in system design

Marek J. Chalupnik, David C. Wynn & P. John Clarkson

Taylor & Francis
Taylor & Francis Group

Comparison of ilities for protection against uncertainty in system design

Marek J. Chalupnik, David C. Wynn* and P. John Clarkson

Department of Engineering, Cambridge University, Trumpington Street, Cambridge CB2 1PZ, UK

The concepts of reliability, robustness, adaptability, versatility, resilience and flexibility have been used to describe how a system design can mitigate the likely impact of uncertainties without removing their sources. With the increasing number of publications on designing systems to have such ilities, there is a need to clarify the relationships between the different ideas. This short article introduces a framework to compare these different ways in which a system can be insensitive to uncertainty, clarifying their meaning in the context of complex system design. We focus on relationships between the ilities listed above and do not discuss in detail methods to design-for-ilities.

Keywords: complex system design; conceptual framework; uncertainty protection; ilities

1. Introduction

Uncertainty – 'the inability to determine the true state of affairs of a system' (Haimes 1998) or 'things that are not known, or known only imprecisely' (McManus and Hastings 2005) – is one of the most fundamental characteristics of engineering design and product development (PD). Several distinct types of uncertainty may be distinguished in PD. For instance, limited machining precision can be described as a source of aleatory uncertainty that can be quantified and considered during design, using probability theory and related techniques. In terms of design organisation, uncertainty is associated with the inevitable surprises that arise when coordinating people and other resources to complete a design. In this case, uncertainty might be considered in terms of the occurrence and impact of events. Other types of uncertainty include ambiguity, for instance in the meaning of language used to describe an emerging design concept, and imprecision, which refers to situations in which the value of a parameter is within a certain range.

Some uncertainty may be described as exogenous to PD (de Weck, Eckert, and Clarkson 2007), for instance arising from organisational change that perturbs established work processes, the instability or unpredictability of demand for a product, changes in user expectations, or the evolution of the political and cultural context of the company (Bstieler 2005). Other PD uncertainties may be described as endogenous (de Weck, Eckert, and Clarkson 2007), because they arise from the inherent novelty of each design and each design process. Endogenous uncertainty is often

---

*Corresponding author. Email: davidwynnemail@gmail.com

increased by product or process technology that is new to a company, and by high complexity in the design process. The latter may be amplified if, for instance, design objectives are technically challenging or there is significant interdependence among subsystems.

The above examples illustrate how uncertainty is prevalent in many aspects of design and PD (see also Thunnissen 2005; Wynn, Grebici, and Clarkson 2011). Due to this multitude of uncertainty types and sources, 'much can and does go wrong' (Wheelwright and Clark 1992). As such, dealing with uncertainty and its effects has attracted a great deal of research attention in PD literature. Many of these studies have focused on ensuring that systems in PD, such as products, processes and organisations, are capable of functioning as intended in the presence of uncertainties. The underlying assumption is that all systems have properties that can collectively be called ilities. Failure avoidance in such systems can be conceptualised as endowing them, by design or designed intervention in the case of an organisation, with ilities that protect against the influence of uncertainty (Crawley et al. 2004). Ilities are systemic properties that arise not only from the parts of a system, but also from the interactions between them. For instance, failures in power grids can be amplified if problems cascade between the interdependent subsystems (de Weck, Roos, and Magee 2011).

Motivated by a high incidence of defects in military electronics systems, much early research in this area focused on controlling product quality in the presence of manufacturing, environmental and user-induced disturbances (O'Connor, Newton, and Bromley 2002). Collectively, these various studies began to form part of the wider challenge of minimising the likelihood of product failure, i.e. improving product reliability. Over the past several decades the concept of reliability has attracted a great deal of attention beyond this original quality control interpretation. For instance, reliability is also an important aspect of system safety, especially in applications such as nuclear power and aerospace engineering where failure carries a high penalty (Petkar 1980).

Research into ilities does not only concern product and production design, but also design process management. As mentioned previously, many sources of uncertainty exist in design, and these contribute to creating schedule risk (Browning 1999). The importance of this has stimulated work on understanding and protecting against uncertainty in engineering projects (e.g. Browning, Deyst, and Eppinger 2002; De Meyer, Loch, and Pich 2002; Yassine 2007).

1.1. *Contribution of this article*

With the increasing number of publications on designing PD systems to have certain ilities, there is also some confusion regarding proper use of these concepts. The lack of clarity arises partly because PD systems such as products and processes vary in nature and have different natural responses to uncertainty and change; the former tend to degrade over time, while the latter actively resist change and maintain themselves. Thus, comparing properties across system types may not always be possible. Nonetheless, much of the conceptual ambiguity surrounding ilities can be attributed to a lack of consensus regarding proper use of the different concepts.

This article argues that certain concepts for protection against the types and sources of uncertainty discussed above can be viewed as different forms of reliability, and placed in a single framework in which different PD systems could be considered. We draw on the literature to select definitions for reliability, robustness, adaptability, versatility, resilience and flexibility that allow these concepts to be clearly related and differentiated within the framework.

Because the focus of the article is to contribute a conceptual framework and not to review the literature on ilities, the literature study is not claimed to be rigorously complete. The framework was developed as follows. Beginning with the commonly discussed concepts of robustness and flexibility, relevant articles were identified in PD-related journals including *Journal of Engineering Design*, *Systems Engineering*, *Management Science* and others. The bibliographies were then

studied and internet search used to locate further relevant sources including PhD theses, conference papers and content from journals that do not have a specific focus on PD. In total, several hundred relevant sources were identified. These were studied to develop the framework in this article. Finally, the set of sources was pruned to create a concise bibliography.

2. Reliability in complex system design

The essence of reliability has traditionally been associated with the 'probability that the system will do the job it was asked to do (i.e. will work)' (McManus and Hastings 2005). This allows for several more specific formulations, some of which are discussed below.

2.1. *Perspectives on reliability*

2.1.1. *Variability-based perspective on reliability*

High reliability has been typically associated with the 'lack of unwanted, unanticipated, and unexplainable variance in performance' (Hollnagel 1993). This perspective is commonly employed in manufacturing, where variability stems from both the manufacturing process and material properties. It is undesirable because it reduces the scope for controlling the products' properties, since unexpected behaviour may be a result of variability arising from manufacture rather than design.

The variability-based perspective on reliability has also been employed in the context of PD processes other than manufacturing. For example, Yassine (2007) conceptualises design process reliability in terms of low variability in process duration. In this context, variability can arise from unpredictable variation, for instance if problems are encountered during a task and some work must be re-done. It can also arise from design decision-making, for instance, because there are several ways of pursuing a particular goal within the process, different routes may be possible according to how participants choose to organise their work.

2.1.2. *Operational environment perspective on reliability*

Defining reliability in terms of minimising variability, as discussed above, is justified in situations where the objective function is of the form nominal-is-better, for instance, because the dimensions of manufactured parts should be as close to the specifications as possible. However, this definition may not always be appropriate. This is because the objective functions for some systems, e.g. process or project execution, include not only predictability but also performance – usually expressed as less-is-better. An example is the desire to absorb adverse effects of uncertainty in a design process so that it may be completed with lower cost and/or shorter duration.

One way of describing the concept of reliability independently from the type of system response is to represent the response in terms of the domains of its operational environment (Zhou and Stålhane 2007):

- Standard Domain (SD), which is the set of all operational conditions for which the system meets its specification.
- Anticipated Exceptional Domain (AED), which is the set of all operational conditions for which the system delivers correct exception outcomes, i.e. meets its exceptional specification.
- Failure Domain (FD), which is the set of all operational conditions for which the behaviour of the system contradicts the specification or the exceptional specification.
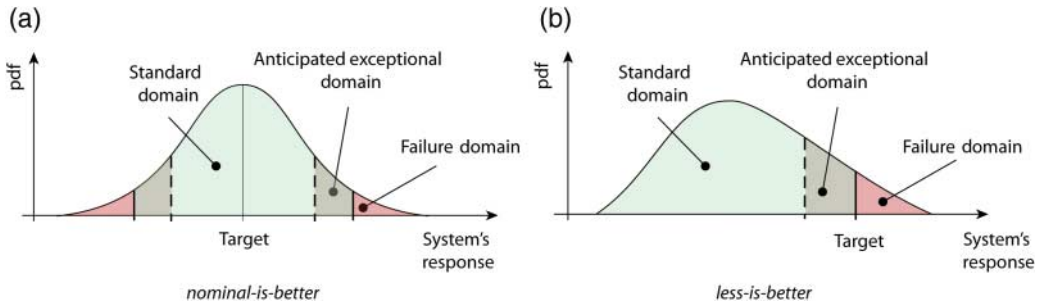
Figure 1. An illustration of the definition of reliability using domains of the system operational environment.

According to this perspective, full reliability is the property of systems with FD = ∅, i.e. the system behaves exactly as specified in its specification and exceptional specification. Decreasing reliability from this probably unattainable optimal point corresponds to an increase in the size of FD.

Figure 1 depicts this definition of reliability by linking the three domains of a system's operational environment to the probability density function (PDF) of the system's response. This allows the reliability of systems with different types of performance targets to be illustrated.[1] Figure 1(a) might be interpreted as the response of a manufacturing process represented as a distribution of the resulting products' characteristics, such as their geometry. In this case, SD signifies all products which result from planned process execution and which have intended characteristics. AED refers to products which are associated with some exceptional but anticipated situations during their manufacture and which also meet the quality specification. FD represents all products that have unacceptable quality characteristics. Figure 1(b) could be interpreted as the duration of a PD process. In this case, SD contains processes that are completed within the planned time frame. AED covers acceptable process durations that reflect some exceptional but anticipated situations and FD denotes unacceptable process durations.

2.1.3. *Failure-mode avoidance perspective on reliability*

A limitation of the traditional interpretation of reliability explained in Section 2.1.1 is that standardised procedures, essential for minimising variance in performance, cannot handle situations for which they were not designed. In other words, these procedures are robust to perturbations that were considered during their design but fragile to unexpected perturbations and design flaws. Although the system operational domains proposed by Zhou and Stålhane (2007) offer a second useful perspective, they suffer from a similar problem – the interpretation of failure depends on the specification of the system operating conditions. Viewing reliability in this way may promote design in which a system has a narrow range of specified operating conditions, and operating the system in unspecified conditions is viewed as misuse that does not compromise reliability.

Given that 'nature does not care what system engineers think the specified operating conditions are' (Clausing and Frey 2005), reliability should ideally be conceptualised in terms independent from the definition of the operating conditions. Clausing and Frey use this argument to conceptualise system reliability as failure-mode avoidance under the full range of conditions that may be experienced. Building on the classification of Zhou and Stålhane (2007) discussed in Section 2.1.2, this full range of conditions can be represented by introducing a fourth domain of a system operating environment to capture operating conditions which are not included in the specification, the Unanticipated Domain (UD), which is defined as the set of all operational conditions which are not included in the system specification. The subset of
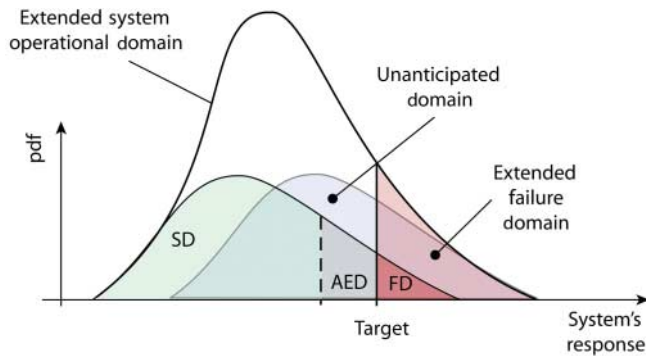
Figure 2. System operational domains, used to explain the perspective on reliability used in this article.

UD that leads to unacceptable system performance can be seen as part of the Extended Failure Domain (EFD). EFD represents the set of all operating conditions under which the system does not meet its objectives. This is illustrated in Figure 2, which shows EFD for a system with less-is-better performance characteristics. Considering all four domains of the system operating environment as one distribution, which may be referred to as the Extended System Operating Domain (EOD), is a useful way of conceptualising the failure-mode avoidance perspective on reliability.

According to this perspective, reliability may be defined as the probability that a system will not fail under the full range of operating conditions represented by SD, AED and UD. In other words, full theoretical reliability can be defined as the property of systems in which EFD = Ø, i.e. the probability that the system will meet its objectives is equal to one.

It is not always possible to predict the evolution of environments in which a system will operate. However, it is possible to develop a better understanding of how that system will behave across different environmental conditions. The essence of improving reliability according to the above interpretation is therefore to extend the set of operational conditions of the system to include more possible environments and system realisations rather than longer time horizons.

Viewing reliability through the perspective of failure-mode avoidance under the full range of operating conditions necessitates an interpretation of reliability that differs from the traditional perspective outlined in Section 2.1.1. This is because specifying the full range of operating conditions is not possible in practice for most PD systems. Therefore, this concept of reliability cannot be interpreted in the quantitative way required by the traditional perspective, and in consequence cannot be measured using traditional metrics such as the number of defects in a batch of products, or the mean time-to-repair. Rather, improving the reliability of a system is to make it fully functional under an increasingly wide range of operating conditions rather than to improve the system's functionality under a specified set of conditions. The importance of employing this perspective is pointed out by Schulman (1996), who notes that to understand the essence of reliability it is necessary to consider what cannot be allowed to happen rather than what happens routinely.

2.2. *Conceptual approaches to improving PD system reliability*

The way in which reliability of a PD system can be improved will depend on the type of that system and its characteristics. However, prior to selecting methods for such improvement, an overall concept for the improvement has to be chosen. Three such concepts are to make the job easier, to reduce uncertainty and to protect the system against uncertainty.

2.2.1. *Make the job easier*

Systems with easier jobs are more likely to meet their objectives. Setting more realistic time targets for a process is one example of this approach. Another example is to set a narrower range of operating temperatures for a product. In Figure 2, this approach corresponds to reducing the extent of EFD by moving the target to the right.

2.2.2. *Reduce uncertainty*

Various uncertainty mitigation strategies aimed at minimising the probability of occurrence of undesired events can be employed. Examples of these approaches include developing knowledge of unknowns, e.g. through additional analyses or testing, and applying risk management techniques. Such approaches are ultimately manifested as reducing the spread of the EFD or reducing the right-hand tail of the EFD in Figure 2.

2.2.3. *Protect the system*

A system can be designed to be less sensitive to various unknowns. As with reducing uncertainty, this results in reducing the spread of the EFD, but system protection is achieved by mitigating not the existence, but the ultimate impact of the uncertainty. There are, in essence, two ways of protecting systems against the impact of uncertainty (de Neufville 2004):

- Active protection. To protect a system in an active way is to ensure, by design, that the system is capable of adapting itself or being adapted to deal with unknowns after they manifest. Ensuring that a system is flexible, i.e. capable of adapting itself to deliver acceptable results despite changes in the target, is one example of active protection.
- Passive protection. Protecting a system in a passive way is to ensure, by design, that the system is capable of withstanding the influence of uncertainty without the need to change its structure or configuration during operation.

   The distinction between active and passive protection for technical systems is related to whether a system can reconfigure itself. For instance, variable wing geometry in aircraft and automatic spoilers in cars may be considered active modes of protection because they allow modification of aerodynamic properties according to need. For socio-technical systems, the difference between active and passive protection can be related to different degrees of managerial involvement (de Neufville 2004).

   While protecting a system is presented here as an alternative to reducing uncertainty, it also involves some uncertainty reduction. This is because knowledge of uncertainties against which the system is being defended is required in order to design the system against them. The uncovering of uncertainties is one form of gaining knowledge and hence also a method of uncertainty reduction.

2.3. *Selecting a conceptual approach for uncertainty mitigation*

In general, the choice of an approach to reliability improvement is constrained in two ways. Firstly, due to competitive pressures, the system's job often cannot be made easier without compromising its attractiveness or value. For example, in the case of a product, reducing its technical specification may result in the deterioration in its perceived attractiveness, and consequently to loss of market share. Likewise, allocating more time to the execution of PD processes will extend time-to-market with similarly adverse effects. Secondly, reducing uncertainty as an approach to

improving reliability of PD systems may be limited due to the fact that some sources of uncertainty are impossible or impractical to reduce (Haimes 1998). An example is the potential change in use of a system over its life cycle.

In light of these observations it is clear that in a majority of situations, protecting the system against the influence of uncertainty is the only practical response.

3. Conceptual objectives for system protection against uncertainty

From the traditional perspective of reliability, systems are considered reliable if they perform as expected in stable environments with stable requirements. However, in the majority of real-life applications, the stability of the environment and requirements cannot be guaranteed. Accordingly a fully reliable system should be protected against the possibility of a changing environment and changing requirements. This section discusses concepts for system protection that approach this objective in different ways and organises the concepts into a framework that clarifies their relationships.

3.1. *Systems with constant requirements*

Protection against uncertainty can be conceptualised as minimising EFD given different interpretations of UD. This subsection considers only one interpretation of UD: unknown operating conditions due to a changing or unknown environment. Two protection objectives based on this interpretation are discussed below.

3.1.1. *Robustness*

3.1.1.1. *Robustness in the literature.* Following the seminal work of Taguchi and Clausing (1990), the concept of robustness has attracted a great deal of attention in PD literature. A variety of system types have been considered, including product, process, project and organisation. Many sources of uncertainty have also been accounted for in the robustness literature, including manufacturing noise, variation in design control variables, uncertain task durations and PD project budget instabilities. Consequently, the concept of PD robustness has many different interpretations. For example, it has been interpreted as a measure of variation in performance (Clausing 1994); insensitivity to anticipated risks (Floricel and Miller 2001); insensitivity to unforeseeable changes in the operating environment (Olewnik et al. 2004); insensitivity to both expected and unexpected variations (Bates et al. 2006); the ability of a system to continue to operate correctly across a wide range of operational conditions (Gribble 2001); the ability of a system to maintain its stated performance level in the presence of fluctuations in primary and secondary inputs, the environment and in human operation (Andersson 1997); the ability of a system to absorb change (Yassine 2007) and the potential for system success under varying future circumstances or scenarios (Bettis and Hitt 1995).

3.1.1.2. *Positioning robustness in the framework.* The understanding of robustness put forward in this article builds upon the extended interpretation of reliability discussed earlier. After McManus and Hastings (2005) robustness is defined as the ability of a system, as built/designed, to do its basic job in uncertain or changing environments. Considering the system operating domains this can be represented as $EFD_P(E) = \emptyset$, where P denotes passive protection and E represents uncertainty in the system's environment (Figure 3).
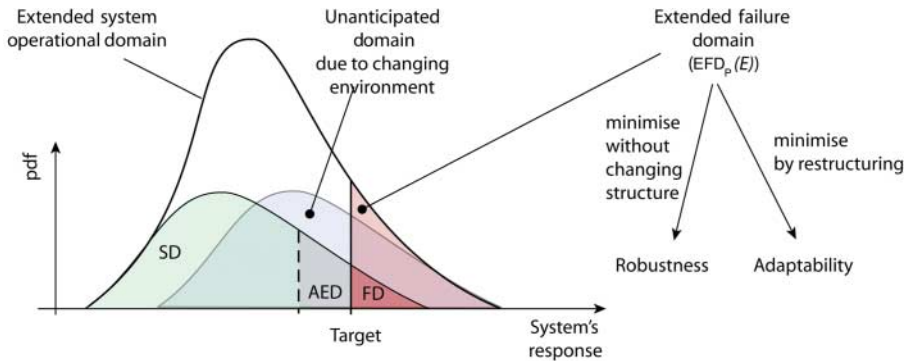
Figure 3. An illustration of robustness and adaptability.

3.1.2. *Adaptability*

3.1.2.1. *Adaptability in the literature.* Adaptability has also been defined in a number of different ways. For example, it has been associated with a system's ability to accommodate predictable changes in operating environment (Olewnik et al. 2004); to exhibit self-organising and emergent behaviour (McCarthy et al. 2006); to be amenable to change to fit altered circumstances (Engel and Browning 2008); to be easily changed to satisfy different requirements (Li, Xue, and Gu 2008) and to change within a given state (Bordoloi, Cooper, and Matsuo 1999). Sometimes, mostly in the context of human–computer interaction, adaptability is distinguished from adaptivity to differentiate between a system's ability to be modified and its ability to modify itself. In the literature of PD, this distinction is less clear. The differentiation between adaptability and adaptivity is thus not considered in detail here.

Whereas major differences among these and other interpretations of adaptability in PD reflect different system types and disciplines, most discussions focus on the notion of change. However, definitions do not agree on or do not pinpoint whether system change is instigated in response to changing requirements and/or changes in the environment.

3.1.2.2. *Positioning adaptability in the framework.* In this article, adaptability is defined, similarly to Fricke and Schulz (2005), as the ability of a system to be modified in order to do its basic job in uncertain or changing environments. Omitting response to requirement change means the definition covers only a subset of the discussions in the literature, but aligns with some definitions and allows the concept of adaptability to be distinguished from that of flexibility in the framework. In particular, this definition of adaptability can be represented as minimising EFD through active protection against uncertainty (Figure 3). For an ideal adaptable system, $EFD_A(E) = \emptyset$, where A denotes active protection.

3.2. *Systems with changing requirements*

Making a system robust or adaptable may improve the likelihood that it will function as intended within changing or unknown environments. To ensure that the system will not fail under a full range of operating conditions, it should also be protected against other sources of uncertainty, which can be represented as changeable requirements. Three conceptual objectives for protection against changing requirements are discussed below.
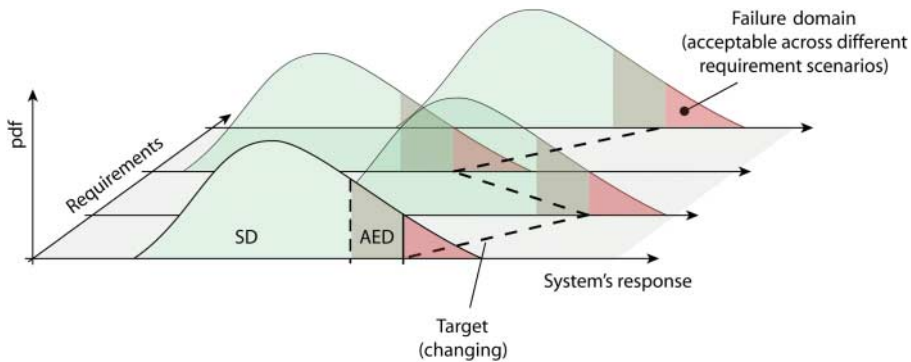
Figure 4. An illustration of versatility.

3.2.1. *Versatility*

3.2.1.1. *Versatility in the literature.* Compared with other ilities, versatility has attracted much less attention in PD literature. It tends to appear as one of many system characteristics, often as a category of, or means of achieving, other ilities such as robustness (e.g. Swan, Kotabe, and Allred 2005) or adaptability (e.g. Gu, Hashemian, and Nee 2004), which are discussed above. In contrast, robustness and adaptability are often discussed in the context of new approaches or paradigms for PD, such as robust design or design for robustness (e.g. Phadke 1989; Taguchi and Clausing 1990) and design for adaptability (e.g. Engel and Browning 2008).

As a consequence of this relative lack of attention, versatility has not been surrounded by the same degree of ambiguity that the concepts of robustness and adaptability have attracted – most authors tend to use this concept in its colloquial sense of multi-functionality. For example, Choi and Cheung (2008) discuss a versatile virtual prototyping system that is capable of meeting requirements of various applications; Braglia and Petroni (2000) view manufacturing versatility as the ability of a firm to switch rapidly from one product type to another; and Haintz and Beveren (2004) define versatile products as those which are multi-functional and offer a multitude of possible experiences.

3.2.1.2. *Positioning versatility in the framework.* We also adopt this focus on multi-functionality and define versatility, after McManus and Hastings (2005), as the ability of a system, as built/designed, to do jobs not originally included in its requirements. Under the operational domain interpretation, versatility can be represented as minimising FD across different requirement scenarios, i.e. $FD(R) = \emptyset$, where R denotes uncertainty in requirements (Figure 4).

3.2.2. *Resilience*

3.2.2.1. *Resilience in the literature.* Intuitively, resilience conveys the notion of bouncing back from adversity (Hale and Heijer 2006) or, more formally, 'the ability of a system to return to its original (or desired) state after being disturbed' (Christopher and Rutherford 2005). While this is one of the most common perspectives of resilience in the literature, many authors interpret it in a broader sense. For example, resilience has been defined as the 'capacity to cope with unanticipated dangers after they have become manifest' (Wildavsky 1988); 'having the generic ability to cope with unforeseen challenges, and having adaptable reserves and flexibility to accommodate those challenges' (Nemeth 2008); 'withstand[ing] a major disruption within acceptable degradation parameters and to recover within an acceptable cost and time' (Haimes, Crowther, and Horowitz 2008); and the ability to absorb and utilise change (Weick, Sutcliffe,
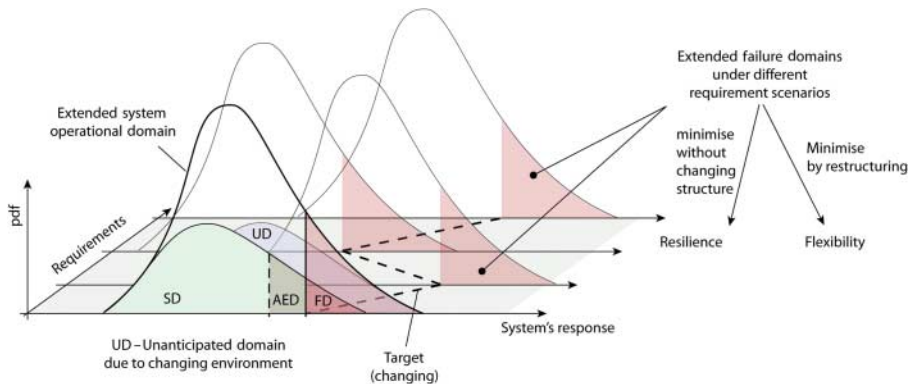
Figure 5. An illustration of resilience and flexibility.

and Obstfeld 1999). Despite the lack of a widely agreed definition of resilience, as illustrated by the above variety of interpretations, most authors define it as one or more of the ability to prevent something bad from happening; the ability to prevent something bad from becoming worse; or the ability to recover from something bad once it has happened (Westrum 2006).

In engineering research, the concept of resilience tends to be used in a narrow sense, focusing on a system's recovery from perturbation (Fiksel 2007). In studies on the resilience of biological, environmental and socioeconomic systems, which dominate the literature of resilient systems, the ability of a resilient system to anticipate and prevent adverse events is often seen as critical (e.g. Woods 2006). However, even introducing this distinction between prevention and recovery does not permit distinction of resilience from similar concepts in our classification. In particular, the above definitions do not discriminate between active and passive system protection.

3.2.2.2. *Positioning resilience in the framework.* We employ a perspective of resilience based on that of Fiksel, who defines resilience as the 'capacity of a system to tolerate disturbances while retaining its structure and function' (2007). According to this interpretation, resilience is a passive mode of system protection that does not distinguish between prevention and recovery. Since the disturbances that are protected against may originate in both the system environment and requirements, we 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. This definition highlights similarities between resilience and robustness. Indeed, the essence of resilience is also to minimise the UD. However, the UD associated with resilience includes changing system requirements in addition to the uncertain environment treated by robustness (Figure 5). This can be expressed as passively minimising EFD across different requirement scenarios, i.e. in the ideal case $\mathrm{EFD_P}(R, E) = \emptyset$.

3.2.3. *Flexibility*

3.2.3.1. *Flexibility in the literature.* Flexibility, which is colloquially associated with 'room for manoeuvring' (Olsson 2006), is one of the ilities most frequently discussed in the literature of PD. Research on flexible systems in PD spans a multitude of systems and perspectives across different domains and is a relatively mature and well-established field compared to other ilities discussed in this paper. Nevertheless, flexibility is still a word rich with ambiguity (Saleh and Jordan 2007). No generally accepted, formal definition of flexibility exists (Bordoloi, Cooper, and Matsuo 1999; Saleh, Hastings, and Newman 2003). Whereas most authors associate flexibility with its intuitive meaning as a system's ability to respond to change (Saleh, Hastings, and

Table 1. A classification of conceptual approaches to system protection against uncertainty.

Concept	Operational domain interpretation	Variable requirements	Variable structure	Variable environment	Active considered	Source(s) of uncertainty
Reliability	$FD = \emptyset$					S
Robustness	$EFD_P(E) = \emptyset$			✓		S + E
Adaptability	$EFD_A(E) = \emptyset$		✓	✓	✓	S + E
Versatility	$FD(R) = \emptyset$	✓				S + R
Resilience	$EFD_P(R, E) = \emptyset$	✓		✓		S + E + R
Flexibility	$EFD_A(R, E) = \emptyset$	✓	✓	✓	✓	S + E + R

Note: S = System; E = Environment; R = Requirements. P denotes passive protection and A denotes active protection.

Newman 2003), the ambiguous nature of flexibility becomes apparent when differences in the interpretation of the change are considered.

To illustrate these differences, consider the following interpretations of flexibility: the ability of a system to handle a wide range of possibilities (Gerwin 1993); a hedge against the diversity of the environment (de Groote 1994); the ability to better meet customers needs (Dixon 1992); the ease of modifying a design to accommodate evolving design requirements (Thomke 1997); the property of systems which can maintain a high level of performance when operating conditions or requirements change in a predictable or unpredictable way (Olewnik et al. 2004); and the property of a product which enables its use in alternative applications (Olsson 2006). Many authors conceptualise different dimensions of flexibility. For example, in the context of production systems, the following types of flexibility have been commonly discussed (Saleh, Hastings, and Newman 2003): volume flexibility; product mix flexibility; new product flexibility; routing flexibility and operation flexibility.

3.2.3.2. *Positioning flexibility in the framework.* Given the objective of this paper, i.e. to position concepts such as flexibility in relation to one another, we do not discuss different types of flexibility in more detail. Instead, we focus on the commonalities and view flexibility as the ability of a system to change its states, i.e. sets of capabilities together with operating conditions (Bordoloi, Cooper, and Matsuo 1999). A system changes its states when its structure is modified to meet new requirements or to operate in a new environment. Accordingly, flexibility can be defined as the ability of a system to be modified to do its basic job or jobs not originally included in the definition of the system's requirements in uncertain or changing environments. This can be conceptualised as actively minimising EFD across different requirement scenarios, i.e. in the ideal case $EFD_A(R, E) = \emptyset$.

4. Discussion

The relationships between the concepts discussed above are summarised in Table 1. As mentioned earlier, the purpose of this article is to clarify and relate the different concepts for system protection against uncertainty, and not to describe methods for endowing a system with these ilities. This is because, we argue, it is important to clearly conceptualise the objective for system protection prior to searching for implementation methods. For further information on the latter, the reader is referred to the relevant articles in the bibliography. A number of conceptual issues regarding system protection in general are highlighted below.

4.1. *Cost of system protection*

The cost of system protection is arguably the most significant barrier to designing high-reliability systems. This cost can manifest in two main ways:

- Endowing a system with an ility usually requires additional resources. For instance, a manufacturing process may require more expensive materials or tools, or a design process may require more time and effort to create a more elaborate design.
- Designing ilities into a system can deteriorate performance. For instance, design for robustness is typically achieved by introducing margins or buffers. Another example is the loss of performance in high-versatility systems, which are less likely to operate across all of their applications as well as their less versatile, application-specific counterparts. In general, this type of cost can be viewed as design opportunities lost due to inefficiencies introduced by system protection.

While it is at least in principle relatively easy to express the cost of protecting a system, calculating potential benefits is more complicated. This is because benefits depend on the perceived importance of the risk that is avoided, which is inherently subjective. Furthermore, these benefits will not be accrued at all if the risk does not materialise. Because a risk is more likely to materialise the longer a system is in operation, there is a trade-off between the short-term cost of implementing uncertainty protection and the possible benefits (Browning and Honour 2008). All of this may render the cost of system protection difficult to justify. In many cases, most stakeholders focus on minimising short-term costs; regulation can play an important role in ensuring that sufficient attention is given to protect against uncertainty and thus manage risk.

4.2. *Relationships between ilities*

The challenges of designing high-reliability systems can be compounded by relationships between the ilities. There are often trade-offs between ilities, such as the inherent conflict between passive and active approaches to system protection (see discussion in Yassine 2007) and the conflict between short-term and life-cycle properties (see discussion in Crawley et al. 2004). Dependency relationships also exist between ilities (Schulz and Fricke 1999; de Weck, Roos, and Magee 2011), for instance, adaptability can be seen as a prerequisite to flexibility. Furthermore, ilities of related systems can interact. For instance, manufacturing flexibility can facilitate design process robustness, because a more flexible manufacturing process allows a wider range of designs to be produced, thereby reducing redesign effort due to unforeseen manufacturing difficulties.

4.3. *Opportunities for further work*

A number of issues are not elaborated in the framework and represent shortcomings as well as opportunities to further develop the conceptualisation.

4.3.1. *Interpretation of a system's basic job*

The basic job of a system is often defined only loosely, leaving considerable freedom for interpretation. As a result, protection against changes to the systems requirements which do not require modifying high-level objectives can be seen as falling within the domain of robustness or adaptability. In contrast, protecting a system against major changes in its requirements will most likely require endowing it with versatility, resilience or flexibility. Future developments of

the framework might include a more detailed description of 'basic job', which would need to be domain-specific.

4.3.2. *Distinguishing between active and passive protection*

Another source of difficulty in classifying approaches to system protection can arise due to the difficulty in defining what constitutes change in structure. For example, exercising a built-in option during process execution could be classified as either passive or active response to uncertainty depending on whether built-in rules regarding process modification are deemed to constitute part of process structure. Likewise, an actuator to change the angle of attack of a compressor vane could be presented as either active or passive protection. Further domain-specific analysis and definitions could strengthen the framework in this area.

4.3.3. *Accounting for human factors in system protection*

Closely related to the built-in flexibility of system structure are various forms of human intervention in socio-technical systems. Because of such intervention, active and passive modes of protection as described in this article may be difficult to distinguish. For example, some mechanisms for system protection may appear active because they depend on unusual human intervention, such as firefighting (see e.g. Schulman 1996 for a discussion on such 'heroic' behaviour in the context of reliability) – even though the underlying structure of the system might seem to remain constant. Furthermore, endowing a collaborative process with ilities is difficult in practice, because human activity systems tend to actively resist change. Further developments of the framework could divide discussion of ilities into systems that incorporate human intervention and those which do not.

4.3.4. *Accounting for uncertainty protection vs. opportunity exploitation*

The framework presented in this article has focused on protection against uncertainty. However, uncertainty entails not only risk, but also opportunity. Of the ilities discussed, systems having higher adaptability, versatility and flexibility are more able to respond to opportunities afforded by uncertainty manifestation than systems designed for passive protection against uncertainty. This is because responding effectively to opportunity usually requires changing the system without incurring significant cost, which is enabled by the above ilities, as well as doing so rapidly, which is enabled by agility (de Weck, Roos, and Magee 2011). Thus, protection and exploitation often require similar characteristics in technical systems. However, the issues are asymmetric when considering process or organisational ilities, because as mentioned above, human activity systems resist deviation, which helps to absorb uncertainty but also hinders positive change.

5. Conclusions

Designing systems such as products, processes and organisations that are capable of functioning as intended despite changes, disturbances and adverse events has been a popular topic in the literature on engineering design and PD. One way of meeting the requirement for systems to operate as intended across a number of different scenarios is, through design, to protect these systems against the influence of different types of uncertainty. Such protection can be conceptualised as design in which systems are endowed with properties called ilities in addition to their basic functionality. This paper has integrated a range of different ilities discussed in the literature

into a conceptual framework which explains the key differences and illustrates the relationships between them. By clarifying the relationships between different concepts for mitigating the influence of uncertainty in PD, the framework is intended to contribute to reducing ambiguity in the description of ilities and, thereby, assist in interpreting and ultimately integrating the approaches aiming to improve them. Because diverse types of PD system are considered within the same framework, the description is necessarily abstract. Further work could develop the conceptualisation by highlighting issues relating to uncertainty protection that are specific to different system types, such as technical vs. human activity systems or long vs. short life-cycle systems. Future research could also extend the framework by classifying ilities and methods to design-for-ilities such as real options (de Neufville 2003), platform modularity (ElMaraghy and AlGeddawy 2012) and Taguchi robust design (Taguchi and Clausing 1990) according to the uncertainty types and sources they can effectively protect against.

Acknowledgements

Note

1. In practice, it is likely that the domains cannot be represented using PDFs as shown in Figure 1 due to fundamental uncertainty about the behaviour of a system; in other words, due to the prevalence of situations in PD where probabilities or distributions cannot be assigned to outcomes due to lack of knowledge of their values, or due to a lack of knowledge that a given event or failure can occur at all. This fundamental uncertainty arises because 'some information does not exist at the decision time because the future is yet to be created' (Dequech 2000). This is particularly relevant in system design, which involves knowledge creation in which each decision that is made reveals or creates new, previously unforeseeable information. Keeping these limitations in mind, this article depicts many concepts using probability density functions as they provide a familiar way to conceptualise the issues discussed.

References

Andersson, P. 1997. "Robustness of Technical Systems in Relation to Quality, Reliability and Associated Concepts." *Journal of Engineering Design* 8 (3): 277–288.

Bates, R. A., R. S. Kenett, D. M. Steinberg, and H. P. Wynn. 2006. "Achieving Robust Design from Computer Simulations." *Quality Technology and Quantitative Management* 3 (2): 161–177.

Bettis, R. A., and M. A. Hitt. 1995. "The New Competitive Landscape." *Strategic Management Journal* 16: 7–19.

Bordoloi, S. K., W. W., Cooper, and H. Matsuo. 1999. "Flexibility, Adaptability, and Efficiency in Manufacturing Systems." *Production and Operations Management* 8 (2): 133–150.

Braglia, M., and A. Petroni. 2000. "Towards a Taxonomy of Search Patterns of Manufacturing Flexibility in Small and Medium-sized Firms." *Omega* 28 (2): 195–213.

Browning, T. 1999. "Sources of Schedule Risk in Complex System Development." *Systems Engineering* 2 (3): 129–142.

Browning, T., J. Deyst, and S. Eppinger. 2002. "Adding Value in Product Development by Creating Information and Reducing Risk." *IEEE Transactions on Engineering Management* 49 (4): 443–458.

Browning, T., and E. Honour. 2008. "Measuring the Life-Cycle Value of Enduring Systems." *Systems Engineering* 11 (3): 187–202.

Bstieler, L. 2005. "The Moderating Effect of Environmental Uncertainty on New Product Development and Time Efficiency." *Journal of Product Innovation Management* 22 (3): 267–284.

Choi, S. H., and H. H. Cheung. 2008. "A Versatile Virtual Prototyping System for Rapid Product Development." *Computers in Industry* 59 (5): 477–488.

Christopher, M., and C. Rutherford. 2005. "Creating Supply Chain Resilience Through Agile Six Sigma." *Critical Eye*, June–August, 24–28.

Clausing, D. 1994. *Total Quality Development*. New York: ASME Press.

Clausing, D., and D. D. Frey. 2005. "Improving System Reliability by Failure-Mode Avoidance Including Four Concept Design Strategies." *Systems Engineering* 8 (3): 245–261.

Crawley, E., O. de Weck, S. Eppinger, C. Magee, J. Moses, W. Seering, J. Schindall, D. Wallace, and D. Whitney. 2004. *The Influence of Architecture in Engineering Systems*. Boston: Engineering Systems Monograph MIT.

De Meyer, A., C. Loch, and M. Pich. 2002. "Managing Project Uncertainty: From Variation to Chaos." *Sloan Management Review*, Winter: 60–67.

Dequech, D. 2000. "Fundamental Uncertainty and Ambiguity." *Eastern Economic Journal* 26 (1): 41–60.

Dixon, J. R. 1992. "Measuring Manufacturing Flexibility: An Empirical Investigation." *European Journal of Operational Research* 60 (2): 131–143.

ElMaraghy, H., and T. AlGeddawy. 2012. "New Dependency Model and Biological Analogy for Integrating Product Design for Variety with Market Requirements." *Journal of Engineering Design* 23 (10–11): 722–745.

Engel, A., and T. R. Browning. 2008. "Designing Systems for Adaptability by Means of Architecture Options." *Systems Engineering* 11 (2): 125–146.

Fiksel, J. 2007. "Sustainability and Resilience: Toward a Systems Approach." *IEEE Engineering Management Review* 35 (3): 5–15.

Floricel, S., and R. Miller. 2001. "Strategizing for Anticipated Risks and Turbulence in Large Scale Engineering Projects." *International Journal of Project Management* 19 (8): 445–455.

Fricke, E., and A. P. Schulz. 2005. "Design for Changeability (dfc): Principles to Enable Changes in Systems Throughout their Entire Lifecycle." *Systems Engineering* 8 (4): 342–359.

Gerwin, D. 1993. "Manufacturing Flexibility: A Strategic Perspective." *Management Science* 39 (4): 395–410.

Gribble, S. D. 2001. "Robustness in Complex Systems." Proceedings of the 8th workshop on hot topics in operating systems, Elmau/Oberbayern, Germany, May 20–23, 21–26.

de Groote, X. 1994. "The Flexibility of Production Processes: A General Framework." *Management Science* 40 (7): 933–945.

Gu, P., M. Hashemian, and A. Y. C. Nee. 2004. "Adaptable Design." *CIRP Annals* 53 (2): 539–557.

Haimes, Y. Y. 1998. *Risk Modeling, Assessment and Management*. Vol. XIII. New York: Wiley.

Haimes, Y. Y., K. Crowther, and B. M. Horowitz. 2008. "Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems." *Systems Engineering* 11 (4): 287–308.

Haintz, C., and J. A. V. Beveren. 2004. "Consumer Adoption of Versatile Products." ANZMAC 2004, Wellington, New Zealand, November 29–December 1.

Hale, A., and T. Heijer. 2006. "Defining Resilience." In *Resilience Engineering: Concepts and Precepts*, edited by E. Hollnagel, D. D. Woods and N. Leveson, 35–40. Aldershot: Ashgate.

Hollnagel, E. 1993. *Human Reliability Analysis: Context and Control*. London: Academic Press.

Li, Y., D. Xue, and P. Gu. 2008. "Design for Product Adaptability." *Concurrent Engineering* 16 (3): 221–232.

McCarthy, I. P., C. Tsinopoulos, P. Allen, and C. Rose-Anderssen. 2006. "New Product Development as a Complex Adaptive System of Decisions." *Journal of Product Innovation Management* 23 (5): 437–456.

McManus, H. L., and D. E. Hastings. 2005. "A Framework for Understanding Uncertainty and Its Mitigation and Exploitation in Complex Systems." Fifteenth annual international symposium of the INCOSE, Rochester, New York, July 10–15.

Nemeth, C. P. 2008. "Resilience Engineering: The Birth of a Notion." In *Resilience Engineering Perspectives: Remaining Sensitive to the Possibility of Failure*, edited by E. Hollnagel, C. P. Nemeth and S. Dekker, 3–9. Aldershot: Ashgate.

de Neufville, R., 2003. "Real Options: Dealing With Uncertainty in Systems Planning and Design." *Integrated Assessment* 4 (1): 26–34.

de Neufville, R. 2004. "Uncertainty Management for Engineering Systems Planning and Design." First engineering systems symposium, Cambridge, MA, March 29–31.

O'Connor, P. D. T., D. Newton, and R. Bromley. 2002. *Practical Reliability Engineering*. 3rd ed. Chichester and New York: John Wiley and Sons.

Olewnik, A., T. Brauen, S. Ferguson, and K. Lewis. 2004. "A Framework for Flexible Systems and Its Implementation in Multiattribute Decision Making." *Journal of Mechanical Design* 126 (3): 412–419.

Olsson, N. O. E. 2006. "Management of Flexibility in Projects." *International Journal of Project Management* 24 (1): 66–74.

Petkar, D. V. 1980. "Setting up Reliability Goals for Systems." *Reliability Engineering* 1 (1): 43–48.

Phadke, M. S. 1989. *Quality Engineering Using Robust Design*. Englewood Cliffs, NJ: Prentice Hall.

Saleh, J. H., D. E. Hastings, and D. J. Newman. 2003. "Flexibility in System Design and Implications for Aerospace Systems." *Acta Astronautica* 53 (2): 927–944.

Saleh, G. M., and N. Jordan. 2007. "Flexibility: A Multi-disciplinary Literature Review and a Research Agenda for Designing Flexible Engineering Systems." *Journal of Engineering Design* 20 (3): 307–323.

Schulman, P. R. 1996. "Heroes, Organizations and High Reliability." *Journal of Contingencies and Crisis Management* 4 (2): 72–82.

Schulz, A. P., and E. Fricke. 1999. "Incorporating Flexibility, Agility, Robustness, and Adaptability Within the Design of Integrated Systems – Key to Success?" 18th digital Avionics systems conference, St. Louis, MO, October 24–October 29.

Swan, K. S., M. Kotabe, and B. B. Allred. 2005. "Exploring Robust Design Capabilities, Their Role in Creating Global Products, and Their Relationships to Firm Performance." *Journal of Product Innovation Management* 22 (2): 144–164.

Taguchi, G., and D. Clausing. 1990. "Robust Quality." *Harvard Business Review* 68 (1): 65–75.

Thomke, S. H. 1997. "The Role of Flexibility in the Development of New Products: An Empirical Study." *Research Policy* 26 (1): 105–119.

Thunnissen, D. P. 2005. "Propagating and Mitigating Uncertainty in the Design of Complex Multidisciplinary Systems"." PhD dissertation, California Institute of Technology.

de Weck, O., C. M. Eckert, and P. J. Clarkson. 2007. "A Classification of Uncertainty for Early Product and System Design." International conference on engineering design, ICED'07, Paris, France.

de Weck, O., D. Roos, and C. Magee. 2011. *Engineering Systems*. Boston, MA: MIT Press.

Weick, K. E., K. M. Sutcliffe, and D. Obstfeld. 1999. "Organizing for High Reliability: Processes of Collective Mindfulness." In *Research in Organizational Behavior*, edited by R. S. Sutton and B. M. Staw, Volume 1, 81–123. Stanford: Jai Press.

Westrum, R. 2006. "A Typology of Resilience Situations." In *Resilience Engineering: Concepts and Precepts*, edited by E. Hollnagel, D. D. Woods and N. Leveson, 55–65. Aldershot: Ashgate.

Wheelwright, S. C., and K. B. Clark. 1992. "Creating Project Plans to Focus Product Development." *Harvard Business Review* 70 (2): 70–82.

Wildavsky, A. 1988. *Searching for Safety*. Piscataway, NJ: Transaction Publishers.

Woods, D. D. 2006. "Essential Characteristics of Resilience." In *Resilience Engineering: Concepts and Precepts*, edited by E. Hollnagel, D. D. Woods and N. Leveson, 21–34. Aldershot: Ashgate.

Wynn, D. C., K. Grebici, and P. J. Clarkson. 2011. "Modelling the Evolution of Uncertainty Levels During Design." *International Journal on Interactive Design and Manufacturing* 5 (3): 187–202.

Yassine, A. 2007. "Investigating Product Development Process Reliability and Robustness Using Simulation." *Journal of Engineering Design* 18 (6): 545–561.

Zhou, J., and T. Stålhane. 2007. "A Framework for Early Robustness Assessment." Eighth IASTED international conference on software engineering and applications, Cambridge, MA, November 9–11.