IEEE Systems Journal, Volume 13, Issue 4, December 2019, pp. 3708-3715
DOI:10.1109/JSYST.2019.2901174

A Resilience Measure to Guide System Design and Management

Timothy L. J. Ferris, *Senior Member, IEEE*

***Abstract*—This paper presents a measure of resilience which can guide system design and management. Systems design must incorporate resilience to provide stakeholders with the most appropriate solution for their life-cycle needs. Design of resilient systems demands a measure of the resilience afforded by a system proposal which can be used to compare design proposals. The measurement method should balance the interest in resilience with all other proposal evaluation criteria, and incorporate the effect of the sequence of unknown future events affecting the system. Ideally, the resilience measure should also be useful to guide management decisions re maintenance or upgrade during the system life. This paper presents a method to measure system resilience which can be applied to engineered systems in general, not just a specific class of systems, is threat type agnostic, and does not presuppose any 'desirable' outcome allowing a system specific determination of 'desirable' outcomes.**

***Index Terms*—Measurement, system analysis and design, system-level design, system metric, systems system resilience**

I. Introduction

RESILIENCE is often discussed in systems engineering but there various interpretations of what it is and this presents a challenge for defining a measure of resilience. In this paper we discuss the concept of resilience in a way that enables a measure of resilience which could be used to compare realized systems, but more importantly, could be used to compare system proposals. Comparison of proposals is necessary to make the measure useful in system design, through answering questions such as: "is this proposal more resilient than that?"

The properties of the measure of resilience presented are:

1. Generalizable to any engineered system.
2. Agnostic of threat type.
3. Agnostic of outcome, both short and long-term, following a threat encounter.
4. Cognizant that performance is multidimensional.
5. Cognizant that threat events occur at any time during the lifecycle, with statistically predictable frequency.

The first property enables use of the measure in system development. For instance, particular systems may require a threshold level of predicted resilience. Generalizability also enables comparison of proposals which may respond differently to each potential threat type.

The second property recognizes that any system operates in an environment with diverse potential threats. Developing protection against one type may make the system more vulnerable to another. Stakeholders who depend on the system are primarily interested in the quality and continuity of service provided rather than the cause of failures.

The third property enables generalization. An acceptable, or desirable, outcome depends on the kind of system. For engineered systems the range of acceptable outcomes is diverse; from virtually no performance glitch, to destruction, and linked to the nature and magnitude of the threat.

The fourth property recognizes that the performance of most systems is multidimensional, and that a single figure measure of performance is rarely meaningful.

The fifth property is important because the probability of threat encounters, of various kinds, is predictable but the time of each encounter, including events affecting the system before recovery or restoration from earlier events, cannot be predicted.

A measure with these properties will accommodate the breadth of concepts of resilience described by Woods [1], namely resilience as rebound, robustness, graceful extensibility, and sustained adaptability.

II. Theoretical Foundations

A. Definition of Measurement

The theory of measurement from Helmholtz [2], through Campbell [3], Bridgman [4] and Stevens [5] to the representational theory of measurement formulated by psychologists [6], and brought into engineering by Finkelstein [7], when extended to provide a relationship of the observed manifestation and the conclusions formed about the observed through the measurement, leads to the definition: "Measurement is an empirical process, using an instrument, effecting a rigorous and objective mapping of an observable into a category in a model of the observable that meaningfully distinguishes the manifestation from other possible and distinguishable manifestations" [8].

This definition depends on the existence of a model of the observed manifestation. The model depends on a definition of the kind of manifestation observed, so, there must be a fundamental link of the measure and definition of resilience.

B. Definition of "Resilience" for Engineering

Resilience scholarship has addressed several system kinds,

Manuscript received XXX/XXX/XXXX.

T.L.J. Ferris is with the Centre for Systems Engineering, Cranfield University, Defence Academy of the United Kingdom Shrivenham, SN6 8LA, UK (e-mail: timothy.ferris@cranfield.ac.uk).

© 2019 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

beginning with Holling's work in ecology [9][10] which focused on restoration of equilibrium after perturbation. Engineering resilience has variously combined time, before, during and after, threat encounters, and outcome kind, such as unimpeded operation or recovery time.

To formulate a model of resilience we must define "resilience" but "it is difficult to identify a single definition that – word for word – satisfies all. However, it is possible to gain general agreement of what is meant by resilience of engineered systems; viz., resilience is the ability to provide required capability in the face of adversity" [11]. Resilience has multiple aspects associated with time before, during and after threat events. The appropriate response depends on both the system and threat specifics.

The state view of system resilience, Fig. 1, which shows resilience as a system property associated with before, during and after threat encounter phases, including damage and performance degradation, was developed to address these difficulties. After degradation the system may be used as it is, fully or partially restored, or decommissioned. Nuss *et al* [12] used an earlier version of Fig 1 to frame their definition of resilience.

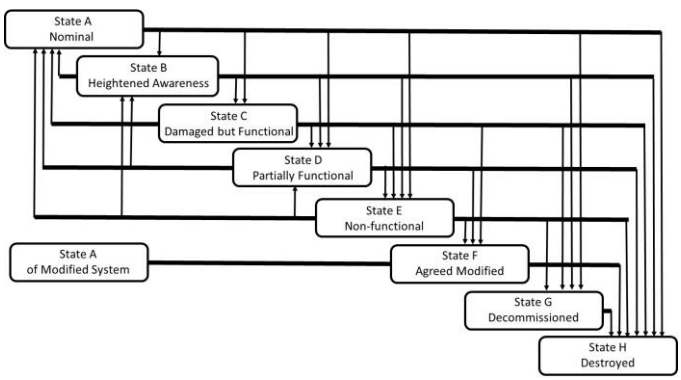

Fig. 1. Simplified system state model of resilience. State transitions that result in the same state before and after the transition omitted.

The state machine view emphasizes that threats may cause system breakage or failure as an engineering fact. Thus, the engineer must determine, and specify, what degradation and restorative possibilities are appropriate in the face of threats. What is appropriate depends on system specifics, so we cannot impose any particular outcome on all systems.

Consequently no measure of resilience that imposes a simple measure, such as time to complete restoration, or time to recover to greater than $x\%$ functionality, is appropriate. The notion of $x\%$ of functionality is problematic because system function is multidimensional [2].

The states in Fig. 1 are summary states which could be expanded to show detail of which system parts are present, functioning or otherwise. Degradation could be modelled by assessing the effect of part failures, singly or in combination. This work could, and should, be done for specific proposals, but cannot be done in general, as applicable to all systems.

III. Review of Measurement of Resilience

We discuss previously published methods to measure resilience.

A. *Unidimensional Measures of Performance or Capability*

Ideally a resilience measure is a single value that represents the achieved system resilience. It would be expected to, at least, describe resilience on an ordinal scale. Preferably, the scale would be of ratio form, enabling direct comparison of amounts of resilience achieved by design proposals [5]. If the measure of resilience is linked to a single measure of performance, then the multiple dimensions of performance must be aggregated to a single measure.

Rehman, Ryan and Efatmaneshnik [13] propose a system capability measure which follows a saw tooth shape through time in response to capability upgrade events. This does not address the multi-dimensionality of the manifestations which lead to capability. Bukowski [14] describes 'performance' using a time function graph of performance. A threat that disrupts causes a rapid, significant, performance diminution followed by recovery, with gradual return to full performance.

Francis and Bekera [15] present a similar unidimensional measure predicated on "the ultimate goal of resilience is the continuity of normal system function". Continuity of normal function may be appropriate for some systems facing certain threat, but this goal should not be uncritically generalized.

Erol, Henry and Sauser [16] present a measure based on a two dimensional disruption probability and consequence severity map of vulnerability to threat types. Erol, Henry, Sauser and Mansouri [17] apply this resilience measurement model in an enterprise scenario discussing several cases *post hoc* without addressing the design phase. They use a single performance variable, achieved to a proportion of design level following Henry and Ramirez-Marquez [18][19]. The same authors [20] applied the concept to power supply recovery after Hurricane Sandy using supply restoration as the singular goal, which is *prima facie* reasonable for a power supply network but is inappropriate for a system where partial performance is meaningful. Their measure is inappropriate if the consumers' premises cannot use supply. Sterbenz *et al* [21] present a similar model to measure remediation strategy effectiveness.

Han, Marais and DeLaurentis [22] plot the percentage of 'full' performance against the percentage of the system which has failed. This approach continues the proportion of performance problem and adds the concept of 'proportion' of the system failure. Uday and Marais [23] recognizes the context specificity of the resilience factors. Disruption and recovery capacity are distinct and what is desirable is system specific, and must be incorporated into a resilience measure. Uday and Marais [24] presented a function of performance level against time, similar to other equivalent resilience measures. Ayyub [25] presents a similar resilience measure, except that the final measure is the time integral of performance as a proportion of design level.

Raj *et al* [26] recognized recovery, rather than failure cause as central to resilience, and provided a resilience measure

relying solely on recovery time. Nan and Sansavini [27] consider a power transmission network providing a resilience measure in the single dimension of actual supply as a proportion of design capacity. This measure assumes the value of achieved performance scales linearly with the quantity. Tran *et al* [28] present a measure using a time integral of performance through events but assume a linear relationship of achieved performance and value. Their method differs from this paper in this and also in using a singular measure of performance.

Hosseini *et al* [29] reviewed definitions and measures of resilience in 2016 finding that there is much diversity and no resolution on both definition and measurement.

The constructs of these measures of resilience do not address the issues 3 and 4 and only weakly address the issues 1 and 5 listed in the introduction of this paper as the desirable goals of a measure of resilience.

B. *Multidimensional Measures of Response*

A societal response to an earthquake is multidimensional and multi-timescale. The approach of [30] is to provide a scorecard where each contributor to resilience is identified but there is no consolidated resilience score. This approach is necessarily *post hoc*. In similar work Van der Beek and Schraagen [31] developed a nine-dimensional scale for the resilience of work teams but provided no unified resilience measure. We note, observation of factors associated with resilience is not measurement of resilience. A similar approach is found in Schneider *et al* [32] which presents a community resilience measure in the face of relevant threats. They identify resilience inputs rather than their effect. These approaches indicate resilience maturity but do not measure resilience.

Tokgoz and Gheorghe [33] present a resilience measure to assess the multidimensional impact of hurricane wind on buildings based on analysis of building wind response. However, they only consider wind threats and not the challenge of multiple threat types.

Wheaton and Madni [34] consider the cost of providing resilience and the potential conflict between solutions offered for different aspects. This is resolved by a trade-off analysis of cost and benefit of possible action. Ross, Rhodes and Fitzgerald [35] present a value model to do the trade analysis starting with a multi-attribute utility calculation using the analytic hierarchy process to combine dimensions. Their approach assists system design and uses a well-understood design trade-off approach. Their approach is limited by its view of resilience as a static problem.

The multidimensional measures of resilience do not address points 3 and 5, and to only weakly address item 1 in the checklist of desired characteristics of a measure of resilience in section I of this paper. The gaps in the desired characteristics of a measure of resilience show that the objective of the measure of resilience presented in this paper is novel. The major gaps between the prior work and the present measure are:

1. The present measure addresses the multidimensionality problem by using the agreed value for scale tradeoff analysis for the system generated for the choice between system alternatives.
2. The present measure uses the statistical distributions of threat events using a Monte Carlo approach to modelling a large plurality of system lifecycles to measure resilience to determine the preferred alternative.

IV. Mathematical Formulations

We consider resilience measures like that presented here.

A. *Brtis Probability Based Metric*

Brtis [36] presents a probability based metric in the first published general purpose measure, as reproduced below.

$$R = \sum_{1}^{n} \left(\frac{P_i}{T} \int_0^T C_r\,(t)_i dt \right) \tag{1}$$

where,

R is the resilience of the required capability C_r

n is the number of exhaustive and mutually exclusive adversity scenarios within a context (n can equal 1)

P_i is the probability of adversity scenario i

$C_r(t)_i$ is timewise availability of the required capability during scenario i. (0 is below the required level, 1 is at or above the required level. Where circumstances dictate this may take on a more complex, non-binary function of time.)

T is length of the mission window

A context can be threat-based or scenario-based.

This metric is based on availability of the threshold value of the "capability", as expressed by the centrality of the term $C_r(t)_i$. This assumes a system only has value if it achieves a performance threshold. If the threshold is closer than necessary to "full" performance in every dimension to achieve a meaningful contribution the metric, R, may be excessively harsh on the proposed system configuration. If the threshold is too low, the metric will insufficiently reflect lost performance. Brtis use of an availability focused, rather than a value-focused measure, is based on concern about the difficulty of a value focused measure to encourage design to improve average performance without focusing on serviceability threshold criteria.

Brtis' metric addresses system capacity to complete a single mission and loses generality because it is tailored for systems used in the episodic manner of 'missions'.

B. *Small* et al – *A Value Focused Thinking Approach*

Small *et al* [37] present an approach with two key categories: Mission Resilience and Platform Resilience. Mission Resilience concerns the mission time-scale, that is episodes of system use with a defined beginning and end. Platform resilience concerns the system life-cycle. Many systems assets are acquired with the intention of significantly long life, during which other stakeholders' actions change

either other assets which interact with the particular system or the scenarios impacting the system. The concept of Platform Resilience was developed in the context of defence systems which have long anticipated life likely to involve the challenges of: interoperability with legacy systems and future systems; component obsolescence; use for unanticipated purposes; and facing novel threats. The acquisition timeline is long, so, even in the absence of other constraints, new assets could not be acquired to respond to the challenges. Other factors, such as cost, result in continued use of assets even when severely impacted by the new challenges.

Small *et al* used value focused thinking (VFT) in a way that overcomes Brtis' criticism. The value of the system is described using the system proposal trade-off process, as normally used in the development of a system to determine which configuration provides the most suitable solution. The trade-off analysis normally involves combining an 'importance' weighting and a value for scale function for each of the multiple attributes. Both the weighting and value for scale functions are agreed before comparing any design proposals. VFT uses the trade-off analysis to compare the value provided by the proposals. If the focus is on alternatives the trade-off is performed with functions that describe the value for scale of achievable measures of the parameters whilst in VFT the range of measures extends to an ideal quantity, and its associated value.

Duirng design ne must choose one of the alternatives offered. In VFT the comparison is made to pre-agreed ideal measures of performance, whilst in threshold based thinking the comparison is with the agreed sufficient value. The effect of this difference is that in VFT the preferred alternative is chosen based on the ideal; any quantity greater than the threshold requirement manifests as either, or both, mission or platform resilience, depending on when its effect is gained.

C. *Nuss* et al – *Resilience as a Tradable Parameter*

Nuss *et al* [12] present a development of an approach to resilience as a tradable parameter in which 'system utility' is calculated through threat events. The method of calculating utility is not developed explicitly, and its value is an aggregate level as a function of time focusing on the mission timescale. This approach addresses goals 1, 2 and 4 of the present measure of resilience. However, there is a fundamental difference because of Nuss *et al*'s focus on recovery, which is nly applicable for some systems, goal 3, and focus on the mission timescale, which is inherently individual sample focused, rather than the lifecycle focus of goal 5, which is, in turn, of greater relevance to decisions about fleets of a system.

V. Proposed Measure of Resilience - Preamble

A. *Foundational Perspective*

The new approach to measuring resilience of an engineered system lies in recognizing the purpose of engineering of systems. Engineered systems are made to provide a service to one or more stakeholders whose primary interest in the system is the service it provides rather than the system itself. A stakeholder who approaches the system as means to an end has relatively little interest in how that service is provided. This observation manifests in the current market for purchase of services rather than assets, but even where the engineered system is acquired, the means to an end it provides is the acquirer's primary interest, not the object itself.

For example, a bus commuter is interested in whether a bus, of roughly the specification they expect arrives and takes them on their planned journey within reasonable schedule, comfort and safety expectations and for the advertised fare. That commuter is not concerned about which bus operates the service so long as the service provider sends one. The service provider sees their bus fleet as means to provide the service, and so long as the fleet can provide the service to agreed expectations their concern with the number of 'spare' buses, under repair or ready to deploy in replacement of a failure, is to have the number that enable them to provide the service at the most profitable level. Technical knowledge of the bus's internal operation is not the interest of either the service operator who uses the buses, or the prospective passenger, who uses the final service provided. The manufacturer of buses is interested in the details of the equipment. Successful manufacturers determine the requirements of the bus in cognizance of the intended service provision.

We observe that the beneficiary stakeholders need the service under certain conditions, but that the service provided may not be useful to them under other conditions. For example, residents of a city which is subject to inundation need a power network which supplies almost all of them at all times, and a reasonable measure of resilience in the face of normal times disruptions, such as vehicle collisions with network equipment, is potentially meaningfully described by duration until all consumers' supply is restored. When an inundation occurs many consumers' premises cease to be fit to receive supply, so supply would be of no benefit. A resilience measure related to the proportion of consumers restored to supply in a specified duration would not be meaningful. A measure of resilience needs to be subtle enough to accommodate the specifics of the system to guide design to provide appropriate outcomes in the face of disruption.

B. *Trade-space as a Method to Resolve Comparative Value*

The conventional systems design approach to decide between multiple design options is to establish a trade-space model to find a figure-of-merit (FOM) for each contending choice. There are several trade-space methods used, each with distinct properties. However, all the methods follow a similar outline, as follows:

1. Identify the set of system attributes or measures which are sufficiently important to be included. This choice is important because an attribute not included in the set will have no influence over the solution chosen, but if the number of attributes is too great the impact of each on the decision is diluted.
2. Determine relative importance weights for each attribute in the set.
3. Determine value-for-scale functions for each attribute in

the set.

4. For each design proposal in the analysis estimate the measure of each attribute likely to be achieved under normal operational conditions. Determine the value of each proposal, usually as the sum of the product of the attribute weights and the value-for-scale of the achievable quantity of that attribute.

The trade-space approach enables a substantially objective comparison of design proposals with different properties across the range of dimensions because the attribute weights and values-to-scale are determined by a staged process where it is difficult to predict the proposal which would achieve the highest FOM. The reader will note that the trade-space approach is not described as objective. This is because the choice of which attributes contribute and their weightings and the values-to-scale result from the expert opinion obtained from subject matter experts and key stakeholders, that is, they are derived from elicitation of opinions.

The fact that the trade-space method for determining which system proposal is preferred is the closest to an objective method makes it appropriate to consider extension of it to measure resilience. We expand this in subsection C below.

C. *Basis of Extension of Trade-space Method for Resilience*

We earlier presented Fig. 1, a state machine model of resilience. There are various definitions of resilience in the engineering literature, all of which are rhetorically clear about the broad content and purpose of engineering resilience but deficient to guide engineering work because they do not provide an actionable framework. The underlying difficulty is that there are too many possible approaches which may be useful in certain circumstances. The first version of Fig. 1 was presented in [38] and [39] and has been redrawn using the conventions of digital bus circuit diagrams to make the relationships clearer. Some other changes have also been incorporated as the authors of the prior works have refined definitions of the states and transitions.

In interpretation of Fig. 1 it is important to note that the eight states are broad-brush states: for example, "State D – Partially Functional", is a broad title that describes many kinds of damage which could have been inflicted on the system and many different impairments of function, including both total loss of certain functions, or diminution in the performance level of certain functions.

It is important to note that Fig. 1 is agnostic concerning the nature of the threat. Systems are subject to various threats, some of kinds anticipated during the design process and others not anticipated, whether or not they should have been. The threat itself does nothing to the system performance. What affects system performance is the system response, or impairment or destruction of some part of the system, resulting from the threat encounter, which in turn affects the system function by not providing the internal service that that part is designed to provide. In turn this leads to impairment or diminution of the capacity of the system to deliver the intended level of service.

From the perspective of the user or beneficiary stakeholders the system provides impaired or, possibly, non-existent, service. Since the beneficiaries are concerned with the system as means to deliver a service their judgement of it depends on the service they receive in the face of threat related events.

We now identify two classes of system, from the perspective of resilience, which will be relevant in development of our resilience measure. The first, and simpler, class is systems required to provide a constant set of functions, each at the same magnitude, under any conditions. The second, more complex class, is where the required functions and performance levels are contingent on conditions, internal or external, because certain capabilities of the system may only be contextually meaningful. For example, a system may have a 'limp home' mode, requiring a lower level of performance of certain core functions than are required for normal operation. The 'limp home' mode may be activated in defined situations. A system must be assigned to one of these classes depending on the system specifics.

VI. Measure of Resilience - Development

A. *Class 1 Systems – Same Performance at all Times*

We begin by developing the figure of merit, FOM, of resilience for systems which are required to have the same level of available performance at all times. At any time, t, the system with n attributes can achieve performance level $P_i(t)$ for the ith performance attribute in the trade-space analysis, as currently used in the design proposal comparison process. The value V_i of the achieved performance level of the ith attribute, $P_i(t)$, is determined using a value-for-scale function, $v_i(x)$, which is the value-for-scale function already determined thin the project for the purpose of trade-space analysis to determine the most desirable alternative:

$$V_i = v_i\big(P_i(t)\big) \tag{2}$$

The weights assigned in the trade-space process, already performed in the project process, are w_i for the ith attribute. Therefore, the instantaneous achieved figure of merit is:

$$FOM(t) = \sum_{i=1}^{n} \Big(w_i . v_i\big(P_i(t)\big)\Big) \tag{3}$$

So the total figure of merit is:

$$FOM = \sum_{i=1}^{n} \Big(w_i . \int_0^T v_i\big(P_i(t)\big).dt\Big) \tag{4}$$

where

T is a meaningful duration of use, either mission or planned lifecycle duration. (A choice is possible so long as all analyses performed in a single comparison have the same interval, T, because decisions about the desirability of system alternatives rely on direct comparability.)

The value of $P_i(t)$ is a discrete function of time, because the system makes step changes of the available performance

depending on event occurrence which may either impair system components, resulting in a lower level of available performance, or transition to State B, where available performance is curtailed by control action in response to awareness of a threat, or restoration to an improved, possibly full design available performance, through repair or the relief of the conditions leading to State B operations.

The duration T can be divided into m intervals such that a monotonic sequence $t_j : j = 0$ to m is generated where $0 = t_0 \leq t_j \leq \cdots < t_m = T$. The times, t_j, are the times when performance diminishing or enhancing events occur. So:

$$\int_0^T \left(v_i\left(P_i(t)\right).dt\right) = \sum_{j=0}^{m-1} \left(v_i\left(P_{ij}\right).\left(t_j - t_{j+1}\right)\right) \tag{5}$$

where

$P_{ij} = P_i(t) \ : \ t_j \leq t < t_{j+1}$

and

$$FOM = \sum_{i=1}^{n} \left(w_i.\sum_{j=1}^{m} \left(v_i\left(P_{ij}\right).\left(t_{j+1} - t_j\right)\right)\right) \tag{6}$$

We break off the development of the resilience measure for Class 1 systems here, to resume in Section C because the development from FOM to MOR is common for both Class 1 and Class 2 systems.

B. *Class 2 Systems – Context Dependent Performance*

In the same way we begin by developing the figure of merit related to resilience for systems for which the required level of available performance is contingent on either environmental conditions, system operating mode or system condition. The same set of n attributes form the basis of system proposal evaluation for each case with distinct available performance requirements. In each of the cases the weightings of the attributes may different, because in the case the need is different, and the value-for-scale functions may also be case specific. Thus, we generate, p, distinct cases, each of which has its own set of weighting factors, which become the matrix with elements, w_{ik}, for attribute i of the set of n, and condition case k of the set of p. Similarly, the values of available performance are determined using the p value-for-scale functions:

$$V_{ik} = v_{ik}\left(P_i(t)\right) \tag{7}$$

The weights assigned in the trade-space process are w_i for the ith attribute. Therefore, the instantaneous achieved figure of merit is:

$$FOM(t) = \sum_{i=1}^{n} \left(w_{ik}.v_{ik}\left(P_i(t)\right)\right) \tag{8}$$

The total figure of merit presented in the development of Class 1, as equation (4), has no analog in the development of Class 2 because the additional concept, the possible transition between required available performance levels following from the operational modes or environmental conditions is a discrete concept.

The value of $P_i(t)$ is a discrete function of time, making step changes of the available performance depending on threat event occurrence which affects the resilience state of the system in Fig. 1. In addition, transition between operational modes or environmental conditions results in changes of the values of w_{ik} and v_{ik}. The values of w_{ik} and v_{ik} change at the same time, and system impairments may happen at any time, in response to threats which affect the system.

The duration, T, can be divided into m intervals such that a monotonic sequence $t_j : j = 0$ to m is generated where $0 = t_0 \leq t_j \leq \cdots < t_m = T$. The times, t_j, are the times when performance diminishing or enhancing events, or changes in operational mode or environment occur. So:

$$FOM = \sum_{i=1}^{n} \sum_{j=0}^{m-1} \left(w_{ik}.P_{ij}v_{ik}\left(P_{ij}\right).\left(t_{j+1} - t_j\right)\right) \tag{8}$$

where

w_{ik} and v_{ik} are the weight and value-for-scale that apply during the interval $t_j \leq t < t_{j+1}$

We break off the separate development of the resilience measure for Class 2 systems here and continue in Section C because the development from FOM to MOR is common for both Class 1 and Class 2 systems.

C. *Transforming Figure of Merit to Measure of Resilience*

Equations (6) and (8) describe the lifecycle, or mission duration, deterministically, which corresponds to the *post hoc* situation of comparing an achieved lifecycle of a single instance of a system. If a system were to operate throughout its lifecycle according to design, with no events that impair its available performance then the FOM would be the same as the design trade-off analysis valuation of that system. Any system impairment, arising from any cause, will lead to an actual FOM less than the ideal. A *post hoc* calculation of the system FOM is not helpful in the engineering development, or system support, because it is only a description of what has been achieved. So we seek a method to assist engineering work.

Resilience concerns the system response to the events occurring through the system lifecycle. These events can be predicted in kind, effect and probability of occurrence, but timing cannot be predicted. The expected FOM for a system through its lifecycle can be determined from the distribution of the FOMs for a large plurality of instances of the design proposal, using the Monte Carlo method to determine values of the t_j, to determine when transitions would happen, and then equation (6) or (8) may be used to determine the FOM for the instance of the lifecycle. The values of t_j can be found by using statistical distributions of the time at which resilience relevant events may occur. The main driving factors are the failure probability of the system elements and the probability of occurrence of the external threats to the system and the nature of the impairments they cause. Restorative transition events occur as a result of maintenance of the system, in

whole or in part, and can be incorporated into the model as distributions of the time to effect repair.

The distribution of the FOM for a single design proposal can be described using descriptive statistics, which can provide understanding the probability of various levels of impairment of the system implemented according to that proposal. A system proposal with desirable resilience characteristics would have a mean and median FOM close to the ideal condition, in which design performance capabilities are always available.

In a design choice between alternatives scenario the FOM distribution for each alternative is determined and statistical tests applied to determine which distribution is better given the decision maker's driving imperatives. Depending on the nature of the system, the mean and median values of the distribution, the distribution dispersion, and the context specific appropriateness of accepting risk a method can be used to select the more appropriate design proposal for the purpose.

VII. Conclusions

This paper has developed a method for determining the resilience FOM for a system proposal based on the constituent elements of the design proposal tradespace process currently used for selection of the preferred design alternative. The tradespace method is well-established, and many variations of that process currently in use could be used in the resilience FOM calculation. Therefore, this approach to determining a resilience FOM allows the continued use of particular tradespace methods already in use, and therefore does not create conflict with those existing methods and the underlying rationale for their application in the particular situations in which they are used. The numerical values of attribute weights and value-for-scale functions which have been determined within a system development project continue to be used in the resilience analyses for the same project.

In a brownfields situation, where action is proposed to change an existing system, or to institute action which would improve the resilience of a system, attribute weights and value-for-scale functions relevant to the proposal will not be pre-existing, because anything that exists relates to the original system which the proposal is intended to change. New values will need to be determined using methods appropriate for the proposed system.

The FOM presented satisfies the original five driving criteria:

1. Generalizable to any engineered system. Any system for which the foundational elements of the tradespace analysis have been developed can be analyzed to determine the FOM. This can be achieved in any greenfield system development project, where the development of the tradespace descriptors is part of the project, and can be achieved for any brownfield project where tradespace analysis is required to determine the relative desirability of each proposal.
2. Agnostic of threat type. The FOM method presented is focused on the achievable performance of the system at any time during its lifecycle, which could be affected by any and all threat kinds, but the analysis is not linked to any assumption about threat types. Specific factors associated with threat types enter the analysis through their resultant system performance measures. Specific threats will cause particular diminutions of performance, or disablement of system elements, which result in changes to performance. Technical analysis of the system and its elements under the influence of those threats is a method of determining the effect of events.
3. Agnostic of outcome, both short and long-term, following a threat encounter. The FOM method accepts as a fact of life that engineered systems cannot be made indestructible, and that any engineered system is subject to impairment, damage and destruction, and that the engineering goal is to provide the system which best achieves the intended effect through the lifecycle. At design time, before the system has been built, the best information available to justify decisions is the statistical knowledge of the kinds of relevant threats and the properties of the elements proposed for use in the system.
4. Cognizant that performance is multidimensional. The tradespace technique is inherently a means of resolving the relative merit of different proposals which addresses the multidimensional character of the observable manifestations of system behavior.
6. Cognizant that threat events occur at any time during the lifecycle, with statistical predictability. Impaired performance resulting from failure is modelled through Monte Carlo analysis enabling comparison of alternatives through analysis of the distributions of FOMs for the alternatives.

The FOM method presented enables comparison of competing design proposals for a system to address a particular purpose. The comparison is based on distributions of the FOM for a large set of hypothesized lifecycles for each design proposal so the selection of the preferred alternative can be based on inferential statistical tests from comparing distributions, using a means of comparison which suits the purpose of the system and the resultant priorities. Development of a resilience measurement as described here enables comparison of design alternatives in system design or system management actions through system life, including decision about the effect of performing, or not performing, maintenance, or possible system modification.

References

[1] D. D. Woods, "Four concepts of resilience and the implications for the future of resilience engineering," *Reliab. Eng. Syst. Saf.*, vol. 141, pp. 5–9, 2015.

[2] H. Helmholtz, *Popular lectures on scientific subjects*, vol. 2. London: Longmans, Green and Co., 1881.

[3] N. R. Campbell, *Physics the elements*. Cambridge, UK: Cambridge University Press, 1920.

[4] P. W. Bridgman, *Dimensional analysis*. New Haven: Yale University Press, 1922.

[5] S. S. Stevens, "On the theory of scales of measurement," *Science*,

vol. 103, no. 2684, pp. 677–680, 1946.
[6] D. H. Krantz, R. D. Luce, P. Suppes, and A. Tversky, *The foundations of measurement*, vol. 1. New York: Academic Press, 1971.
[7] L. Finkelstein, "Theory and philosophy of measurement," in *Handbook of measurement science theoretical fundamentals*, vol. 1, P. H. Sydenham, Ed. Chichester: John Wiley and Sons, 1982, pp. 1–30.
[8] T. L. J. Ferris, "A new definition of measurement," *Measurement*, vol. 36, no. 1, pp. 101–109, 2004.
[9] C. S. Holling, "Simplifying the complex: The paradigms of ecological function and structure," *Eur. J. Oper. Res.*, vol. 30, pp. 139–146, 1987.
[10] B. Walker, C. S. Holling, S. R. Carpenter, and A. Kinzig, "Resilience, adaptability and transformability in social-ecological systems," *Ecol. Soc.*, vol. 9, no. 2, 2004.
[11] "System resilience," *Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 1.9*, 2017. [Online]. Available: http://www.sebokwiki.org/wiki/System_Resilience#Definition. [Accessed: 25-Jun-2018].
[12] A. J. Nuss, T. D. Blackburn, and A. Garstenauer, "Toward resilience as a tradable parameter during conceptual trade studies," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3393–3403, 2018.
[13] O. U. Rehman, M. J. Ryan, and M. Efatmaneshnik, "Future proofing process," in *27th Annual INCOSE international symposium*, 2017.
[14] L. Bukowski, "System of systems dependability - Theoretical models and applications examples," *Reliab. Eng. Syst. Saf.*, vol. 151, pp. 76–92, 2016.
[15] R. Francis and B. Bekera, "A metric and frameworks for resilience analysis of engineered and infrastructure systems," *Reliab. Eng. Syst. Saf.*, vol. 121, pp. 90–103, 2014.
[16] O. Erol, D. Henry, and B. Sauser, "Exploring resilience measurement methodologies," in *INCOSE international symposium*, 2010.
[17] O. Erol, D. Henry, B. Sauser, and M. Mansouri, "Perspectives on measuring enterprise resilience," in *IEEE International systems conference*, 2010, pp. 587–592.
[18] D. Henry and J. E. Ramirez-Marquez, "A generic quantitative approach to resilience: a proposal," in *20th Annual International Symposium of the International Council on Systems Engineering*, 2010.
[19] D. Henry and J. E. Ramirez-Marquez, "Generic metrics and quantitative approaches for system resilience as a function of time," *Reliab. Eng. Syst. Saf.*, vol. 99, pp. 114–122, 2012.
[20] D. Henry and J. E. Ramirez-Marquez, "On the impacts of power outages during Hurricane Sandy - a resilience-based analysis," *Syst. Eng.*, vol. 19, no. 1, pp. 59–75, 2016.
[21] J. P. G. Sterbenz, E. K. Cetinkaya, M. A. Hameed, A. Jabbar, S. Qian, and J. P. Rohrer, "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation," *Telecommun. Syst.*, vol. 52, pp. 705–736, 2013.
[22] S. Y. Han, K. Marais, and D. DeLaurentis, "Evaluating system of systems resilience using interdependancy analysis," in *IEEE international conference on systems, man, and cybernetics*, 2012, pp. 1251–1256.
[23] P. Uday and K. Marais, "Resilience-based system importance measures for system-of-systems," *Procedia Comput. Sci.*, vol. 28, pp. 257–264, 2014.
[24] P. Uday and K. Marais, "Designing resilient systems-of-systems: a survey of metrics, methods, and challenges," *Syst. Eng.*, vol. 18, no. 5, pp. 491–510, 2015.
[25] B. M. Ayyub, "Systems resilience for multihazard environments: definition, metrics, and valuation for decision making," *Risk Anal.*, vol. 34, no. 2, pp. 340–355, 2014.
[26] R. Raj, J. W. Wang, A. Nayak, M. K. Tiwari, B. Han, C. L. Liu, and W. J. Zhang, "Measuring the resilience of supply chain systems using a survival model," *IEEE Syst. J.*, vol. 9, no. 2, pp. 377–381, 2015.
[27] C. Nan and G. Sansavini, "A quantitative method for assessing resilience of interdependent infrastructures," *Reliab. Eng. Syst. Saf.*, vol. 157, pp. 35–53, 2017.
[28] H. T. Tran, M. Balchanos, J. C. Domercant, and D. N. Mavris, "A framework for the quantitative assessment of performance-based system resilience," *Reliab. Eng. Syst. Saf.*, vol. 158, pp. 73–84, 2017.
[29] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 47–61, 2016.
[30] Committee on Increasing National Resilience to Disaster Hazards and Committee on Science Engineering and Public Policy, *Disaster resilience: national imperative*. Washington, DC: The National Academies Press, 2012.
[31] D. van der Beek and J. M. Schraagen, "ADAPTER: analysing and developing adaptability and performance in teams to enhance resilience," *Reliab. Eng. Syst. Saf.*, vol. 141, pp. 33–44, 2015.
[32] J. Schneider, C. Romanowski, R. K. Raj, S. Mishra, and K. Stein, "Measurement of locality specific resilience an operational model," in *IEEE international symposium on technologies for homeland security*, 2015.
[33] B. E. Tokgoz and A. V Gheorghe, "Resilience quantification and its application to residential building subject to hurricane winds," *Int. J. disaster risk Sci.*, vol. 4, no. 3, pp. 105–114, 2013.
[34] M. J. Wheaton and A. M. Madni, "Resiliency and affordability atributes in a system tradespace," in *AIAA SPACE 2015 Conference and Exposition, AIAA SPACE Forum, (AIAA 2015-4434)*, 2015.
[35] A. M. Ross, D. H. Rhodes, and M. E. Fitzgerald, "Interactive value model trading for resilient systems decisions," in *Procedia computer science Conference on systems engineering research*, 2015, pp. 639–648.
[36] J. S. Brtis, "How to think about resilience in a DoD context," Colorado Springs, CO, 2016.
[37] C. Small, G. Parnell, E. Pohl, S. R. Goerger, B. Cottam, E. Specking, and Z. Wade, "Engineered resilient system with value focused thinking," in *27th Annual INCOSE international symposium*, 2017.
[38] S. Jackson, S. C. Cook, and T. L. J. Ferris, "Towards a method to describe resilience to assist system specification," in *25th annual INCOSE international symposium*, 2015.
[39] S. Jackson, S. C. Cook, and T. L. J. Ferris, "A generic state-machine model of system resilience," *INCOSE Insight*, vol. 18, no. 1, pp. 14–18, 2015.

Timothy L.J. Ferris (M'91–SM'02) received the degrees B.E.Hons, University of Adelaide, 1982, B.Th., Flinders University, 1988, B.Litt.Hons., Deakin University, 1991, GradCertEd, Queensland University of Technology, 2002, and PhD, University of South Australia, 1997. His PhD was in the theory of measurement.

He worked as an engineer for Electricity Trust of South Australia and Morrison Court Pty Ltd, and in the Presbyterian Church before commencing as a lecturer at University of South Australia, 1991. He is currently working in the Centre for Systems Engineering, Cranfield University, Defence Academy of the United Kingdom Shrivenham, UK. He has published about 150 papers in journals and conferences and various other items.

Dr Ferris was Secretary, IEEE South Australia Section (2004-2005), is an Associate Editor of *IEEE Systems Journal*, and was Publication Chair, *SoSE 2014* conference. He is a member of INCOSE.

Cranfield University

CERES Research Repository **https://dspace.lib.cranfield.ac.uk/**

Cranfield Defence and Security Staff publications (CDS)

A resilience measure to guide system design and management

Ferris, Timothy L. J.

2019-03-18

Attribution-NonCommercial 4.0 International

Timothy L. J. Ferris. A resilience measure to guide system design and management. IEEE Systems Journal, Volume 13, Issue 4, December 2019, pp. 3708-3715
https://doi.org/10.1109/JSYST.2019.2901174

Downloaded from CERES Research Repository, Cranfield University