Analysis of resilience situations for complex engineered systems – the resilience holon

Rachel Freeman, Liz Varga

***Abstract*—Improving the resilience of complex engineered and engineering systems (CES) includes planning for complex resilience situations, in which there may be multiple threats, interactions, and disruptions. One challenge in the modeling of CES is the identification of how interactions in a complex situation occur and their combined influence on CES resilience. This paper presents a resilience holon that can be used to analyze complex resilience situations. It is made up of 24 elements (defining types of resilience, threats, interactions, and disruptions), which have varying importance to specific situations. Holons can be linked together hierarchically or in a network. An application of the resilience holon to a documented real-world resilience situation, widespread flooding in a city, illustrates its use. Pathways taken by threats and disruptions, as the flood effects cascaded through the city, are shown as connections between holons. The resilience holon could be used to decompose diverse resilience situations involving CES, to identify where critical vulnerability points are and how the whole resilience situation could be improved. The visual nature of the resilience holon could be used in an interactive way, allowing stakeholders to better understand the full resilience picture of CES that they use or operate.**

***Index Terms*—Complex engineered systems, threats, disruptions, interdependencies, infrastructure systems, resilience, holon**

I. INTRODUCTION

One key factor in improving the resilience of complex engineered and engineering systems is understanding complex resilience situations, in which there may be multiple threats, interactions, and disruptions. The term complex engineered or engineering systems (CES) [1] includes both: (i) complex systems that are engineered, being the outputs of engineering activity – such as railway networks, power plants and computers; and (ii) complex systems that carry out engineering, being the capability systems that design, manufacture, operate, supply, maintain, and decommission engineered systems – such as the organizations that build or maintain rail networks.

Recent decades have seen huge improvements in reliability and safety engineering; for example, in Japan road traffic deaths were reduced by around three quarters between 1966 and 1984 [2]. However, CES are becoming increasingly complex and interconnected, more difficult to manage, and simultaneously more essential to everyday life [3]. Complexity can arise from structural complexity (size, connectivity, architecture), dynamic complexity (short term, long term), and socio-political complexity [4]. Additionally, the variety of types of threats to CES continues to grow – such as climate change impacts, malicious cyber-attacks or physical threats, and resource constraints [5]. Two examples of CES failures follow: During Hurricane Sandy in 2012 in the USA, "lifeline infrastructure sectors were severely compromised due to a lack of investment in mitigation measures and inadequate planning for managing cascading disruptions across interdependent systems" [6]; The failure of a water system in Italy in 2009, after an earthquake, was due to poor levels of critical functionality (robustness, redundancy, resourcefulness, rapidity of response) in both soft and hard infrastructure systems that made up the network [7].

A. Resilience and the research gap

Resilience has been defined in several ways, including: "A process linking a set of adaptive capacities to a positive trajectory of functioning and adaptation after a disturbance" [6]; Different responses to "changes in the relationship between open dynamical systems and their external environment" [8]; "The ability to anticipate possible adverse scenarios/ events…prepare for them, withstand/absorb their impacts, recover from disruptions caused by them and adapt to the changing conditions" [9]. Different ways of measuring resilience exist, for example: As an uncertainty-weighted resilience metric that is based on "three resilience capacities: adaptive capacity, absorptive capacity, and recoverability" [10]; As a "resilience profile" which indicates how sensitive a system is to different types of errors or threats [11]; As a "method for ranking critical components in interdependent infrastructures" [12].

Improving resilience is covered in the literature from numerous angles, for example: Value of Information analysis can be a means for resilience management, and used to increase service life benefits through Structural Health Monitoring [13]; Resilience can be improved through understanding the tradeoffs between vulnerability reduction and recoverability enhancement [14]; Resilience can be seen as a multi-objective optimization problem, with "simultaneous objectives to maximize survival probability, maximize reactive timeliness, and minimize the total budgeted cost" [15]; Resilience engineering proposes that four abilities are necessary for resilient performance: responding, monitoring, learning and anticipating [16]. Resilience can be incorporated into system architectures, for example: A conceptual framework identifies four key domains that require investment, to build the resilience of essential services – technical and social resilience that is specific (to particular risks) or general (capacity to deal with novel risks) [17]; Ross and Rhodes describe methods for architecting and designing systems products, and services that can deliver value robustness in a changing world [18].

There have been calls for improving both the framing and the analysis of the resilience of CES. The first part of this challenge is in recognizing that resilience is not always a fixed attribute. Resilience can be seen as an epistemological property of the system, versus an inherent one [10]. Whether being resilient is a tangible or intangible capability will depend upon the context, and there is a need to untangle the complexities involved [19]. The second part of the challenge is in improving tools to deal with real-world complexity and uncertainty. Resilience in practice incorporates a wide variety of situations, and a resilient organization under a regular threat may not be resilient under an "unexampled event" [20]. Existing risk analysis methods do not allow systems with high complexity and interconnectedness to be adequately modeled; the full spectrum of threats cannot be taken into account, nor can dynamic or even non-linear behavior be handled, nor changes in contextual factors [3]. Risk analysis modeling, "must evaluate consequences for each risk scenario as functions of the threat (initiating event), the vulnerability and resilience of the system, and the time of the event" [21]. There is a need to "work with the reality that CES often change over time, developing new features, and evolving to meet changes in their operating environment" [1].

B. *Terms related to resilience*

Hazards have been defined as "a process, phenomenon or human activity that may cause loss of life, injury or other health impacts, property damage, social and economic disruption or environmental degradation" [22]. Hazards are characterized by their location, intensity or magnitude, frequency, and probability. Hazards have four types of origin: (i) Natural hazards are associated with natural processes, including extreme weather events such as tropical cyclones, floods, droughts, and heatwaves; (ii) Anthropogenic hazards are caused by human activities and decision making; (iii); Technological hazards arise from industrial conditions, dangerous procedures, infrastructure failures or specific human activities; (iv) Socio-natural hazards are a result of combined natural and anthropogenic factors, including climate change (adapted from [22]). Hazards can be seen as the sources of threats.

Threats and risks are hazards that manifest in a particular way or location. Threats are more general; risks are more specific to particular CES or locations. Threats have three aspects: their predictability, their potential to disrupt a system, and their origin [20]. Threats can be regular (frequent enough for systems to develop a regular response), irregular (infrequent but known events), and unexampled (completely unexpected) [20]. Risks can be emergent related to technology, linked to interconnectedness, or slow-developing [23]. Technology-related risks can arise as uncertain impacts from science and technology innovation, dependencies in technological systems, and when known technologies are used in different contexts [24]. Risks can be classified as "acceptable", "tolerable but in need of reduction", or "intolerable" [25]. For example, civil engineers can consider the benefits and costs in preparing for a 1 in 100 year flood event versus a 1 in 10 year event. Slow-developing risks follow a pattern in which slow, hidden changes are not addressed until a point of rapid and sometimes irreversible change occurs [26]. Risk management planning is common practice in the construction and management of CES, and across government. "Benchmarks and thresholds for risk analysis are built into the regulations and policies of organizations and nations" [27]. Risk registers identify particular risks, estimating their likelihood and potential threats (for example, the UK Climate Change Risk Assessment [28]).

Several trends are expected to increase threats to CES in future. For example, the likely effects of global warming above 1.5°C include increasingly extreme weather events that affect CES operating conditions [29]; the number of electricity users at risk of flooding is expected to double in the UK due to climate change [28]; increasing interactions between the biosphere and the technosphere will create new types of challenges [30].

Disruptions and perturbations are the effects on CES of manifested threats. Perturbations include external changes that have potential to interfere with the normal functioning of a system; they can be induced by ecological, economic or political changes [31]. Disruptions have been described as "natural or man-made, external or systemic, single agent or multi agent, and short-lived (i.e. transient) or enduring" [32]. Disruptions can be differentiated between those that affect a single infrastructure and those related to infrastructure interdependence, with the second type being failures to confine disruptions to the first type [33]. Disruptions to critical infrastructures can be distinguished as accidental or intentional [3]. Disruptions in supply chains are described as a change that affects the structure of a network and its future functionality [34]. The increasing interconnectedness of critical infrastructure services presents potential for widespread disruptions, since they are "mutually or circularly dependent and involve distributed complex physical and cyber networks" [35].

C. *Resilience situations*

In discussing a typology of resilience situations, Westrum notes the existence of commonalities in the "threats that resilience protects against and the modes in which it operates" [20]. The concept of a resilience situation is key to this paper, and illustrated in Fig. 1. Key elements are:

(i) CES structures, including capital stocks (e.g. buildings, equipment) and organizational structures;

(ii) The functionality of CES, including operations required to meet CES performance requirements;

(iii) The expected outputs of CES, being the value that CES provide in goods and services;

(iv) The unexpected (unwanted) outputs from CES, such as gaseous or material outputs that are harmful to the environment and society;

(v) The useful inputs needed by CES, such as energy, water, feedstocks, finance and human resources;

(vi) Operating conditions for CES, including weather conditions, access to critical services, and regulation;

(vii) External risks in the operating environment, when operating conditions are not those expected;

(viii) Internal risks that can arise within CES, such as the risk of operator errors;

(ix) Manifested threats, which are those risks that actually occur;

(x) Interactions between CES resilience profiles and threats;

(xi) Disruption effects from threats not dampened by the resilience profile and additional interactive effects.

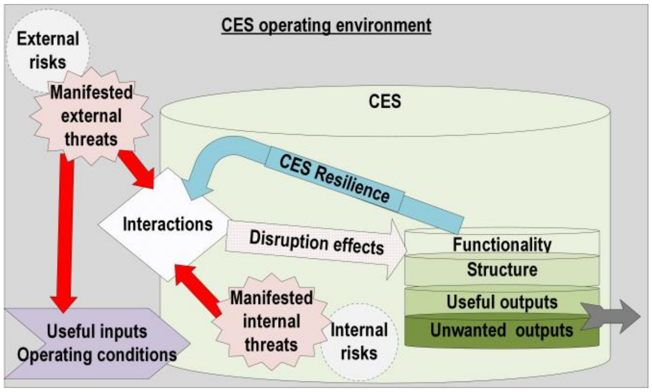

Fig. 1. Depiction of a resilience situation. The resilience profile of the complex system mitigates some of the effects from manifested threats – either internal or external or both. Disruptions may affect system functionality, structure, or inputs and outputs.

D. *Study scope*

In response to calls for improving the framing and analysis of the resilience of CES, this paper presents a new lens with which to view resilience in CES – the resilience holon. It is a tool for identifying key factors and interactions that can guide actions to improve resilience in a situation. It is designed to be simple enough to be applicable to a wide variety of resilience situations, and detailed enough to provide specific findings. It could be used during ex-post analyses of CES failures; in ex-ante studies that aim to prevent disruptions; to analyze legacy systems that have been adapted or added to over their lifetimes; and to look at the resilience of new systems that form part of the 4th (cyber-physical) industrial revolution.

The benefits of the resilience holon are in improving: (i) the boundary setting for resilience studies; (ii) disaggregation of the observed accumulated and/or combined effects of multiple threats; (iii) the setting of priorities when investing in the resiliencing of CES; and (iv) the provision of evidence for comprehensive risk registers and risk management plans. Intended audiences include: (i) those working on the resiliencing of CES through complexity modelling, conceptual or theoretical studies; (ii) those managing or designing CES; (iii) those managing or operating in the engineering supply chain; (iv) those responsible for managing societal risk in government; and (v) those teaching about resilience in the engineering discipline.

The paper outline is as follows: Section 1 introduces the intent and scope of the paper and terminology used; Section 2 describes the resilience holon; Section 3 applies the resilience holon to a case study of a resilience situation with interdependency; and Section 4 provides conclusions and suggestions for future work.

II. The Resilience Holon Concept

A. *Holons*

The term holon was first described by Koestler [36] as a "modeling scheme for autonomous entities that can consist of other, smaller autonomous entities" [37]. Holons present both a face showing a self-contained whole and another face showing a dependent part – in other words, holons are simultaneously both a "whole" and a "part" ([36] from [38]). Holonic architectures are structures made up of holons in a hierarchical manner, usually described as a "holarchy" (originally from [39]). The idea of holonic architecture has been applied to many aspects of systems engineering and enterprise governance, including sensor networks [40], management of traffic [41], and in the design of distributed manufacturing systems (e.g. [42], [43]). Examples of resilience studies using holonic architecture include the design of resilient networked critical infrastructures [44], and a resilience assessment project to understand critical infrastructure interdependencies in Toronto [45]. Holonic architecture is similar but different from the concept of systems of systems (SoS), which are "large-scale, integrated, complex systems that can operate independently but are networked together for a common goal" [46] (from [47]). While interactions between sub-systems in SoS can lead to complex behaviors, and indicators of resilience may differ between system levels [17], the concept of systems of systems does not necessarily imply hierarchy.

B. *Resilience holon definition*

The resilience holon is proposed as a means to represent and analyze resilience situations. The resilience holon represents a self-contained resilience situation, which can stand on its own or be connected to and dependent upon other resilience holons. The focus on analyzing resilience situations means that the structure and/or function of CES may not be represented in the same way that most SoS analyses do. In contrast to holarchies, the concept of holons is used here without assuming a hierarchy of holons exists – although it may do in some cases.

To define a resilience holon, seven core attributes are required to exist in the real-world situation being represented. Attributes one to four are tangible and their identification is part of usual practices in the design and management of CES. Attributes five to seven are less tangible and will require definition through, for example, expert judgment, defining resilience indicators with ordinal scales, or ex-post analysis of CES failure case studies. The core attributes are: (i) Engineering structures and/or people structures. (ii) One or more useful outputs (e.g. for a bridge the output is the safe passage for travelers over a terrain). (iii) One or more inputs needed for functionality of CES (e.g. bridge maintenance, chemical feed-stocks). (iv) One or more hazards, threats, or risks that can or do impact the structure and/or function of CES. (v) The resilience profile of CES that describes likely responses to potential threats. (vi) Disruptions and/or threat responses. (vii) Interactions between CES resilience profiles and manifested threats.

Fig. 2 presents the structure of the resilience holon. There are four groups of elements in the resilience situation – disruptions, interactions, threats, and resilience profile – making a total of 25 elements. These groups were chosen based on the key elements in a resilience situation as shown in Fig. 1, and are explained in detail in the following sub-section (II C). Structure and functionality of CES (shown in Fig. 1) are not represented directly, but indirectly through the values in the resilience profile. In other words, the resilience holon needs only to identify how structure and functionality respond to threats, and not the details of what the structure and functionality are.

Elements in the four groups are uniquely identified by a letter and number combination: the group they are in is a letter (R=resilience, T=threats, I=interactions, D=disruptions) and then elements are numbered incrementally. There may be more than one threat, interaction, or disruption in a resilience situation – indicated by the labels 1 to n, 1 to p, and 1 to q (the number of each may not be the same). The arrows between the groups indicate the relationships between the groups. The threats, resilience profile and disruptions groups interact via the interactions group. Interactions can go both ways, shown by the dual direction arrows.

In a typical situations the threats group and resilience profile group will interact with each other, and produce disruptions; the arrow between interactions and disruptions would be unidirectional. However, in more complex situations, disruptions can feed back to create additional threats that interact with the resilience profile. Hence, arrows connecting interactions to disruptions, threats and resilience profile go in both directions.

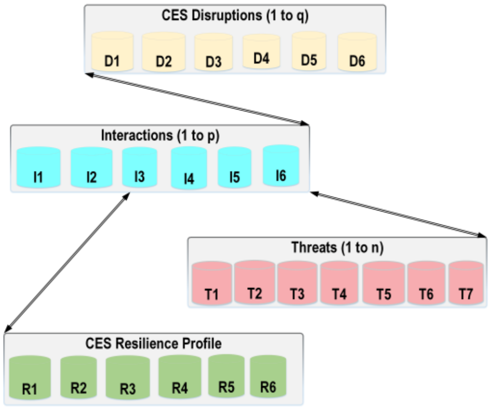

Fig. 2. Structure of the resilience holon.

C. *Resilience holon elements*

1) Resilience profile group

The resilience profile identifies six core capacities that contribute to overall resilience. It is based partly on notes from an expert workshop[i], and partly from the framework for resilience analysis in Francis and Bekera [10]. Their framework names three major capacities that make up a system's resilience capacity: (i) Absorptive capacity is the "degree to which a system can absorb the impacts of system perturbations and minimize consequences" [10]. (ii) Adaptive capacity is the ability of a system to change in response to negative impacts, which can happen when there is insufficient absorptive capacity [10]. (iii) Restorative capacity can be measured by the speed at which systems return to normal operations and system reliability [10].

Resilience capacities can be related to the concept of "ilities" used in systems engineering - "e.g., availability, maintain-ability, vulnerability, reliability, supportability, etc." [48]. For example. Enos [49] relates the ilities to resiliency; adaptability, extensibility, flexibility, repairability, and versatility are identified as achieving resiliency for engineered systems in defense programs. The resilience profile does not include ilities directly, but some of the capacities are aligned with ilities.

R1 Design margin: (Absorptive capacity) Design margins are "the extent to which a parameter value exceeds what it needs to meet its functional requirements" [50]. Similar terms include: resilience margin [51], safety margin, assurance margin, future growth margin, product flexibility margin, and design excess margin [50]. Margins indicate that system usage and evolution can be marginally outside of expected operating conditions without impacting system functionality. Wide design margins can mask system stresses, however, meaning the observed performance of a system may not always reflect its health and stability, and operating too close to design limits for a length of time can create vulnerability to failure.

R2 Dampening: (Absorptive capacity) CES that are able to dampen perturbations can stop threat effects from continuing after threats have ceased being active, or spreading beyond the initial threat location. One of the aims of resilience engineering is to prevent systems inadequately responding to perturbations [52]. If threat effects do multiply and spread, CES can eventually become destabilized enough to cause failure or state changes.

R3 Risk-knowledge and planning: (Adaptive capacity) Identifying, planning for, and reducing exposure to risk is a core resilience practice. It requires up-to-date knowledge of existing and potential future risks, assessing their size and likelihood, and putting in place plans for reducing risk exposure. Strong centralization of risk planning across a network, or a focus on very stringent targets for reducing exposure to risk, can make systems less agile and less able to match risk management to particular locales.

R4 Fidelity of system knowledge: (Adaptive capacity) Fidelity, or the level of realism, of knowledge about a system is critical when adaptive responses to threats are required, providing vital knowledge about where faults might be found and what options are available. A lack of fidelity can happen due to increasing system complexity, changes in workforce, and not documenting changes during system evolution. Cyber-physical technologies can improve system knowledge; however, too much reliance on them can mean faults remain hidden, and knowledge of the history of a system is disregarded.

R5 Redundancy and variety: (Restorative capacity) Redundancy means that more than one option for provision of physical and/or organizational capacity is available, which can be used when failures occur or additional capacity is needed. Using up redundancy can improve cost efficiency but reduce restorative capacity. Ashby's law of requisite variety [53] indicates that a system's ability to respond to variety in its operating environment increases with the variety within the system. Reducing diversity within a system could remove stabilizing balancing feedback mechanisms.

R6 Recoverability: (Restorative capacity) Recoverability is the "ability of the system to recover in a timely manner" [14], also defined as the restorative capability [54]. Similarly, repairability is "the ability to be returned to the original state of function when some function is lost" [49]. Of concern are the amount of time needed to restore functionality, and the need for replacement of parts of a system to achieve restoration. In networks, the concept of a "repairability envelope illustrates trade-offs for counter-measures against cascading failures" [55]. Recoverability is important for all systems but speed of recovery is vital for critical infrastructures.

2) *Threats group*

T1 Changes to inputs: Unwanted changes to required inputs can affect system functionality, and also system structure if certain inputs are needed to maintain a system. Examples of regular inputs that can change and threaten systems include: supplies of raw materials and parts; critical services such as water, power, energy, information and communication technology (ICT) networks, and data storage; availability of workforces with particular skills, availability of transport networks.

T2 Frequency, synchronicity: The frequency with which threats occur, and their synchronicity with other threats, can change the severity of threats through combinatorial effects. When threats occur with high frequency there is less time for restoration of the system to normal operations between threats. Synchronicity between threats can increase the overall size of effects. Risk prevention procedures that have been put in place may be insufficient if they assume a short-lived threat event.

T3 Internal: Internal threats are those that arise within organizations that build or run CES; they can occur during any of the life-cycle phases of CES. Examples include: operator errors, failures of maintenance, failure to abide by safety regimes, high staff turnover leading to a loss of expertise, failure to train new staff, insufficient robustness in engineering design.

T4 External: External threats arise in CES operating environments. They must be distinguished from normal (expected) conditions, such as expected passenger flows in a rail network, expected availability of materials during the building of infrastructure, expected ambient temperature. Extreme outliers from normal conditions are low probability conditions that may become threats.

T5 Speed of impact: The speed at which threats arise affects CES responses. Some arise slowly and there is enough warning to prepare, while others occur almost without any warning. An earthquake (without seismic monitoring) provides almost no time in which to prepare. Slower growing threats can be forecasted, such as a predicted heatwave which will stress electricity grids – also categorized as slow-developing catastrophic risk [26].

T6 Regularity (how well known): Threats can be regular, irregular, or unexampled (outside of the "collective experience envelope" [20]). In general, the less a threat is known, the more likely planning will be inadequate. Known threats may not be preventable, but engineers can design systems to be "safe to fail" [56]. The regularity of threats changes over time; for example, many threats seen early on in the industrial revolution have now been eliminated. Predictions for unexampled future threats exist, such as unplanned for emergence between mass cyber-physical systems.

T7 Size: Threats can be relatively small compared to the size of CES and easily dealt with, or very large compared to CES. For example, losing a small percentage of the supply chain to a manufacturing plant would not seriously affect production in a system with good absorptive capacity, but losing a key supplier could lead to a production shutdown until supplies are restored, as happened due to flooding in Thailand in 2011[ii].

3) *Interactions group*

I1 People-technology interactions: There are constant interactions between technologies and operators and users, in most CES. Competency in people-technology interactions eventually becomes automatic after a period of learning, but operating complex systems may require more conscious control compared to simpler technologies [57]. CES failures may be a sign that "too much complexity has been allowed into the system for most of us (or perhaps even anyone) to understand" [58].

I2 Compounding: Threat effects can be compounded if threats occur close together in time or location, or when low-lying but constant threats weaken a system and then other threats occur. Interactions can increase the total size of simultaneous threat – often referred to as a "perfect storm". Examples include: "King tides" caused by the position of the moon and the time of year[iii]; electricity brownouts due to very hot weather causing high power demand, combined with unplanned power station outages and low efficiency in the power stations still online[iv].

I3 Cascading: Cascading describes a situation when a disruption in one sub-system causes a disruption in one or more connected (sub)systems [59]. Cascading has been observed in major historic power outages in electricity grids [60], and in inland waterway infrastructure disruptions when there was loss of a key asset [61]. In connected systems, a breaker that prevents disruptions from spreading can save lives and infrastructure assets [12]. High reliability theory [62] aims to prevent the cascading effects of threats, but it can reduce the benefits of interconnectivity too.

I4 Autocorrelation: Autocorrelation describes second-order interactions between the effects of threats. The effects of threats combine over time, causing increasing instability and variance in a system's response to new threats. As variance and autocorrelation increase, systems take longer and longer to return to their former state and critical slowing down occurs [63]. In ecosystems, autocorrelation increases as the system moves toward a critical (often unwanted) state transition [64].

I5 Emergence: Emergence is "higher order effects resulting from the complex interaction of multi-fold individual components and the combination of multiple non-linear and reinforcing effects" [65]. Emergence can be difficult to observe in early stages, since interactions may remain unseen until higher order effects start to affect functionality. Emergence can occur when control and monitoring of systems is highly automated and decisions are not tempered by human judgment, such as in smart city sensing infrastructure [66] and in electric business processes [67].

I6 Interdependency: Interdependencies in infrastructure can be physical, cyber, geographic, or logical, and are dependent on coupling effects, and response behaviors [68]. Recovery from situations with interdependency can be slow; for example, recovery from black sky events (a prolonged electricity outage over a substantial area) could take up to a week [69]. Interdependency can be mutual, such as highways requiring power for traffic control and power systems requiring highways for access to distributed power infrastructure. Interdependency can be a strength, such as when one networked sub-system compensates for another that has failed.

4) *Disruptions group*

D1 Increased vulnerability: CES may be structurally, organizationally or financially weakened after disruptions have occurred. Repeated cycles of threats and recoveries can reduce the resources needed for improving resilience, such as financial and workforce resources, meaning the system is left more vulnerable until a full recovery can be achieved (if this is possible).

D2 Structural loss or damage: Structural loss can happen to hard systems and/or people systems. Damage to hard systems is seen when physical capital is made useless or seriously damaged [70]. Structural loss can range from: minor damage that weakens structures over time but leaves them functioning; to damage to particular parts of the structure that can be isolated and then repaired; to catastrophic loss of the whole structure. Damage to organizational structures are harder to identify but can be seen in high staff turnover, loss of expertise, or weak leadership.

D3 Loss of useful outputs: Loss of useful outputs can range from: degraded or substituted output of goods or services; to a loss of output of goods or services for limited but planned periods of time; to a complete loss of useful outputs for an indefinite time. A mitigation strategy for dealing with threats can include allowing reduced performance for a limited time in order to keep services going, as described in the taxonomy of management [71].

D4 Financial losses: Financial losses can be caused by any combination of the five other types of disruptions, or can be purely financial. Examples of financial losses include: required increased spending on reducing vulnerability, required investment to restore structures that have been damaged, reduced income from loss of useful outputs, the requirement to pay compensation when harm to people occurs, and the payment of fines or clean-up costs for harm to the environment.

D5 Harm to people: Harm to people from CES can take many forms, such as ill health due to local pollution; fatalities or injuries from CES failures; loss of vital services such as power or water; or loss of shelter when homes are made inhabitable. The harm to people depends on the criticality of CES, which ranges from not critical, to increasingly critical infrastructure-like, to critical. Society's vulnerability to threats increases with "increasing reliance on large, complex systems for critical infrastructure services" [70].

D6 Harm to region, environment: Harm to the region or environment can range from: little to no environmental harm, some lasting environmental damage which can be cleaned up within months to years, up to decades or more of severe environmental harm, possibly at the global scale. Examples include the death of marine life from a toxic waste spillage at sea, and the release of long-lasting nuclear pollution after a nuclear power accident. Emissions of greenhouse gases from the combustion of fossil fuels can be seen as a very slow-acting, global-scale disruption.

D. Use of the resilience holon

The resilience holon can be applied singularly to the whole resilience situation, or recursively, breaking down the situation into many resilience holons. The number of holons depends on what level of detail is needed to fully characterize the situation. To link holons, a disruption (or threat response) from one holon can be a threat (or resilience response) for another. Multiple holons could be arranged as a flat structure, such as a network, or as a hierarchical structure – or some combination of both. The challenge for those using the resilience holon to analyze a resilience situation, will be to create an arrangement of holons that provides new and useful understanding but without becoming too complex in itself.

One issue in this approach is the setting of resilience holon boundaries. Complex systems modeling tends to define sub-systems along boundaries that are operational, technological and/or organizational. The resilience holon provides an opportunity to define boundaries of analysis that align with resilience situations that are seen in the design and management of real-world CES. With this increased freedom, however, comes the need to establish a new rationale.

At a minimum, all seven core attributes described in section II.B should be identifiable in some form within the boundary. At a maximum, the holon boundary should incorporate so many elements that the resilience situation cannot be understood. Holon boundaries may or may not be proportional to the size of sub-systems. For example, there may be a particular part of the system that is small in size but highly influential on the resilience situation. Or quite large sub-systems might be combined into a single holon, if splitting into smaller holons would provide no additional benefits in understanding the resilience situation.

The process of breaking down a resilience situation, to provide a suitable level of detail, could be done through iterative decomposition. For example, by first identifying a small (e.g. less than 5) number of influential resilience holons which, combined together in an arrangement, represent the whole resilience situation; and then continuing with further levels of decomposition where needed. This process would be similar to the decomposition method used in Hierarchical Process Modelling [72].

Adding further details to the resilience holon arrangement, elements in each resilience holon can be defined to be important, or not, to the situation; eliminating the need for further consideration of unimportant elements. Importance can be positive (reducing disruptions) or negative (increasing disruptions). Threat and disruption elements are assumed to always be negative (although in rare cases, a disruption could end up reducing disruptions by chance). Resilience and interaction elements can be positive or negative. A simple visual method to mark importance is to assign color coding to each element. Another method, where there are numerous holons, is to create a table that relates resilience holons and the elements in them.

III. Case study application of the resilience holon

This section uses the resilience holon to analyze a real-world resilience situation: an incident of flooding in Lancaster, UK. The incident was analyzed in detail by Kemp in [73] and [74]. River flood barriers were breached due to exceptionally high rainfall, and a distribution grid substation was flooded and went offline, meaning a loss of electricity throughout the city; there was a loss of internet and mobile signals due to both infrastructure being flooded and loss of electricity; roads were flooded and there was a loss of public transport; thousands of homes and businesses were flooded. The effects on everyday life were highly disruptive for the whole city: normal electronic communication channels between people and organizations stopped working; banking was unavailable; shops were unable to process credit card payments; public service information was unavailable through broadcast media (until one local radio station found a way to broadcast) and few people had devices to pick up media without internet; disruptions to water supplies in high buildings; loss of study days at Lancaster University and schools; direct harm to people (especially vulnerable people including the homeless and those in nursing homes); loss of income to businesses; stress on emergency services; and many other effects too numerous to list. The floods of the winter of 2015 to 2016 were estimated to have cost £1.6 billion (over the whole north west of the UK, which includes Lancaster) [75].

A. A resilience holon for the whole resilience situation

Fig. 3 shows the resilience situation as a resilience holon, with the boundary set to encompass the river flood barrier breach and the cascading effects on the whole city. Elements that are important to the situation are colored, and those with little relevance are in white. All elements in the interactions, threats and resilience profile groups that are colored are negative, contributing to disruptions.

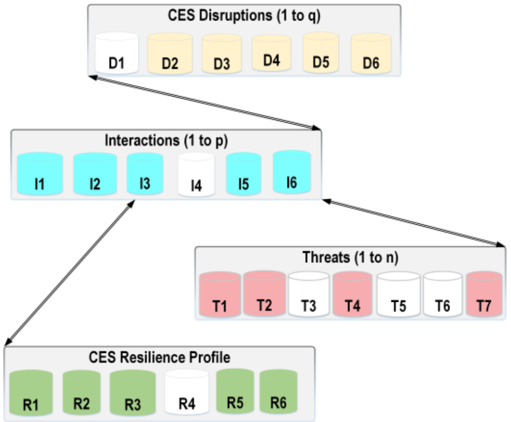

Fig. 3: Example resilience situation represented as a resilience holon – flooding in Lancaster, UK. Elements not important to the situation are colored white.

The elements with color are explained as follows:

R1 Design margin: Although flood defenses had been built to protect the city, they were not high enough to prevent the river overtopping. Thus, the design margin was insufficient to deal with the very high amount of rain that fell in a short time. **R2 Dampening**: The flood water was not controlled and prevented from spreading from the area close to the river to the rest of the city. **R3 Risk-knowledge and planning:** while flooding was a known risk, there was insufficient risk management in place to deal with the loss of critical services and the secondary effects. **R5 Redundancy and variety:** A lack of redundancy was seen in many areas affecting everyday life, but most importantly in communications and finance. There was a lack of alternative devices such as land-line phones, wind-up radios, or established in-person networks to stand in for mobile phone and internet communication; many people were unable to buy groceries due to a lack of cash or shops unable to run cash registers. Emergency services have their own communications systems, which were unaffected, and the hospital had its own backup generators with fuel supplies. **R6 Recoverability:** Emergency services were stretched to restore critical services and clear roads, but power was restored to the whole city after a week. Emergency generators were brought in from other areas in the first few days, allowing some restoration of power.

T1 Changes to inputs: Flooding was caused by extreme rainfall patterns, with 300mm of rain from storm Desmond; at the peak, the river Lune had the highest flow ever recorded for a river in England [74]. **T2 Frequency, synchronicity:** Part of the reason for flooding was that the ground was already waterlogged due to high rainfall in the previous month. **T4 External:** The threat came from outside the city's control. **T7 Size:** the size of the rainfall was much higher than planned for when flood barriers were built.

I1 People-technology interactions: People were unable to use many technologies they were reliant on, especially for communication, and used non-technological methods instead such as going door to door or posting notices in windows. **I2 Compounding:** the loss of electricity, information, and supplies compounded the negative effects, especially for those with flooded homes or businesses that needed to make quick decisions in a crisis. Emergency services were hampered by blocked roads and loss of power. One fire station had to close, as it was flooded. **I3 Cascading:** The initial threat spread from a high flowing river, to damage to the substation, to failure of many different critical services. **I5 Emergence:** Many people found ways to communicate using whatever methods were available. One local radio station continued to run, getting information by someone going to another city that had internet and mobile signal, and relaying it via a landline. The hospital was visited by people wanting to get a hot meal and charge electronic devices. **I6 Interdependency:** The most impactful interdependency was between the electricity grid and ICT networks (both public and private). Water pumping to high-rise buildings was affected leaving some without water.

D2 Structural loss or damage: Many buildings and their contents were badly damaged by floodwaters, also vehicles and roads. **D3 Loss of useful outputs:** Useful outputs from almost all of the city's businesses and transport networks and the university and schools were affected. **D4 Financial losses:** Large financial losses were seen by a wide variety of individuals, the public sector, and businesses; losses were both in loss of income and in high clean-up costs. Insurance companies faced large payouts. **D5 Harm to people:** Everyone in the city was affected during the flood, but especially people in vulnerable situations with insufficient resources; students lost a week of studies. **D6 Harm to region, environment:** Flooding tends to move items like vehicles and debris around, sometimes including toxic waste. This has to be cleared up although the damage is usually not long lasting.

Elements without color are explained as follows: **D1 Increased vulnerability:** the resilience and structure of the city was not permanently weakened. **I4 Autocorrelation:** no secondary responses were seen that increased the strength of the threat over time. **T3 Internal:** the threat did not arise within the city. **T5 Speed of impact:** the water deluge happened quickly but not suddenly, and there was time to attempt to restrict the flooding with sandbags (unsuccessfully). **T6 Regularity (how well known):** the flooding risk was well known. **R4 Fidelity of system knowledge:** there was prior knowledge of the risk to the transformer and the town's infrastructure.

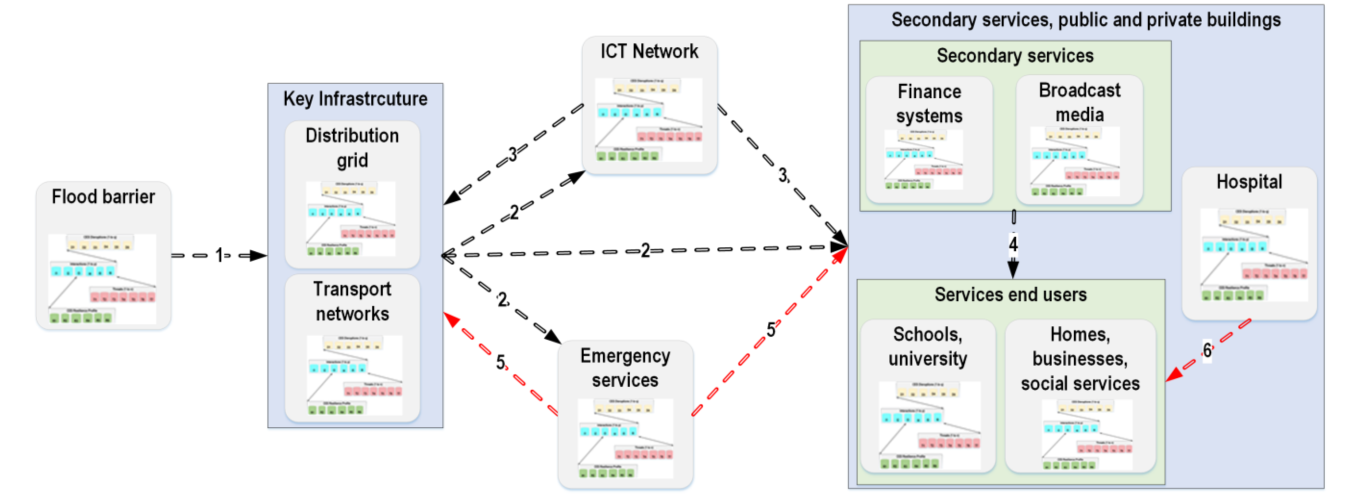

Fig. 4: Resilience situation of flooding in Lancaster, UK, decomposed into an arrangement of resilience holons. Element colors have not been adjusted as in Fig. 3; instead Table I identifies the important elements in each resilience holon.

TABLE I: IMPORTANCE OF ELEMENTS IN THE CASE STUDY RESILIENCE SITUATION SHOWN IN FIG. 4

	Flood barrier	Transport systems	Distribution grid	ICT systems	Emergency services	Secondary services	Hospital	Services end users
R1 Design margin	x	x	x				y	
R2 Dampening	x	x	x					
R3 Risk-knowledge & planning	x	x	x	x	y	x	y	x
R4 Fidelity of system knowledge					y			
R5 Redundancy and variety		x	x	x	y	x	y	x
R6 Recoverability	x	x	x		y		y	x
T1 Changes to inputs		x		x		x		x
T2 Frequency, synchronicity	x				x			
T3 Internal								
T4 External	x	x	x	x		x		x
T5 Speed of impact		x	x	x		x		x
T6 Regularity (how well known)				x	x	x	x	x
T7 Size	x	x	x		x			
I1 People-technology interactions				x		x	x	x
I2 Compounding		x		x	x			
I3 Cascading		x	x	x	x			
I4 Autocorrelation	x							
I5 Emergence						y	y	y
I6 Interdependency		x	x	x	x	x		x
D1 Increased vulnerability		x						x
D2 Structural loss or damage	x	x	x					x
D3 Loss of useful outputs	x	x	x	x		x		
D4 Financial losses		x	x	x		x		x
D5 Harm to people		x		x		x		x
D6 Harm to region, environment	x							

B. *Multiple resilience holons in a structure*

Since the majority of elements in Fig. 3 are colored, it is difficult to discern any new insights except that it was a major event for the city. To gain more insights, the situation is broken down into an arrangement of ten resilience holons (Fig. 4). They are arranged in a partially hierarchical structure, going from the highest to lowest level, from left to right. Holons with similar behaviors are grouped together. Note: The transport networks holon includes the local road, rail and bus networks, and direct flooding of buildings via roads. Holons represent both the physical systems and the people running or using them. Thus, the holon labeled "services end users" includes the majority of the public in Lancaster.

An arrow from one holon to another indicates that a disruption (negative) or resilience response (positive) in the first holon actively influences the second holon, as, respectively, a threat (negative) or improved response (positive). For example, the disruption caused by the failure of the flood barrier became a threat to key infrastructure; the resilience response in emergency services enabled the recovery of key infrastructure.

The arrows joining holons in Fig. 4 are numbered from 1 to 6, and colored red if it is a resilience response. They are explained as follows: (1) Disruption as failure of the flood barrier became a threat to the distribution grid and transport networks. (2) Disruption in the distribution grid and transport networks (including direct flooding of buildings) became threats to the whole city. (3) Disruption in ICT systems as lack of internet access and mobile phone signals became a threat to the functioning of secondary services, end users of services, and the recovery of key infrastructure. (4) Disruption in secondary services became a threat to services end users. (5) A resilience response from emergency services eventually brought key infrastructure back into functionality, and helped the rest of the city to recover and/or temporarily cope. (6) The hospital provided temporary support for some individuals.

To add further detail, the most important elements in each resilience holon are identified in Table I. Those elements that contributed to disruptions are marked with an "x", and those that helped to reduce disruptions are marked with a "y". While the unselected element/holon combinations could be active, the table highlights which are judged to be the most important ones in the resilience situation. For this initial test of the resilience holon, table assignments were made with the authors' personal judgments based on details in the post-event report [74]. However, in a real world setting, they would ideally be made with input from a broad range of stakeholders; which is especially important in multi-agency settings.

The initial event, the failure of the flood barrier, is fairly straightforward to understand – a larger than expected threat overcame insufficient design margin, risk knowledge, and ways to dampen after effects. Fig. 4 and Table I illustrate how secondary effects from the initial event cascaded throughout the city. In terms of improving resilience, each resilience holon is a self-contained resilience situation which could be examined to improve its resilience profile. In addition, the whole resilience holon arrangement shows pathways of threats and disruptions as the flood waters affected the whole city. Some interactions reduced disruptions. Two holons with positive resilience responses were the emergency services and the hospital, which mostly continued to function as expected, due to good resilience profiles that had been put in place due to the critical nature of their operations. Some temporary positive emergence was also seen in responses from the public who found ways to communicate using non-digital methods, and at the hospital in providing additional services not usually offered.

The shape of Fig. 4 highlights ICT systems as a critical point in the resilience situation, with many secondary effects from the lack of ICT provision. Only the emergency services were largely able to continue without ICT systems since they had their own independent communication systems. One approach to reducing secondary effects would be to improve ICT systems resilience. In this analysis, however, the resilience profile is not particularly bad; it is just that without electricity there ICT systems cannot function. Providing redundancy in the form of an alternative electric supply to ICT systems, for example, would improve resilience but would be unlikely to be economically justifiable (as noted by Kemp [73, p108]). In other words, there is a limit to the realistically achievable resilience in ICT systems. Accepting that ICT systems may fail during extreme events implies a need for more redundancy in secondary services and for the end users of services, through non-digital methods. This would partially reduce inter-dependency on ICT systems, at least temporarily. For households and businesses who do not typically do risk planning, and for the university that hosts students on campus, more help and advice could be provided on ensuring non-digital resources and communication networks are available when needed.

The holonic view of the Lancaster flood presented in Fig. 4 and Table I is an initial trial of use of the resilience holon. It provides a broad view of the flood event and, on reflection, it aligns well with the key findings from Kemp's analysis of the event [74]. It is not, however, well enough developed to produce notably counterintuitive findings. Further development could include reviews by stakeholders and systems engineers, and quantifying the values in Table I with weighting factors that reflect their relative contribution to the resilience situation.

To summarize this section, a resilience holon has been defined, with guidance on its use to analyze resilience situations. A case study of its application to a real world event illustrates its potential for examining resilience situations.

IV. Conclusions and further work

The resilience holon can be used to analyze resilience situations involving CES. It is designed to be generic enough to be applicable to most real-world situations, yet detailed enough to provide useful and novel insights. The resilience holon is applied to a documented real-world resilience situation, as a case study. The key difference between the resilience holon and other resilience concepts is the focus on complex resilience situations involving CES. When threats and disruptions are endogenized within the resilience situation view, it is possible to identify resilience situations in which the same core elements under different stresses can lead to different kinds of outcomes.

The paper contributes to closing an acknowledged research gap in resilience studies. The first challenge is to understand whether resilience is a tangible or intangible capacity of system(s) [19], in other words whether it is situation dependent or not. We cannot comment on the general situational dependency of resilience in CES, but the resilience holon provides a way to approach resilience in CES from the perspective of situation dependence.

The case study illustrates this by describing a complex system that was, in theory, at low risk of widespread failure. A flood barrier had been built to protect the city and the city had a highly reliable electricity supply and ICT networks. The particular context of the situation was much higher than expected rainfall over several weeks, combined with high reliance on electricity and ICT systems for essential daily activities. The context meant that the resilience profiles of some parts of the city, represented as holons, were insufficient to prevent harm. Disruptions went beyond the direct effects of flooding, with secondary disruptions impacting basic services for city residents and businesses. The context for resilience might have been different. For example, had the city not had such usually reliable services some redundancy might have been left in the system to cope with failures; had those managing risk for the distribution grid considered the failure of the flood barrier to be sufficiently likely, they might have moved the substation to higher ground.

The second challenge is to improve the modelling of CES that have high complexity and interconnectedness, including the full spectrum of threats, dynamic or non-linear behavior, and changes in contextual factors. The resilience holon provides a way to map out resilience situations in a form that includes numerous threats, non-linear behaviors, and high interconnectedness. Resilience holons can be arranged to reflect key parts of a resilience situation, how they interact, and how threats and disruptions might spread or be restricted through improved resilience. The visual nature of the resilience holon could be used in an interactive way, to allow stakeholders to build conceptual models of resilience situations and communicate the narrative to others. Additionally, systems with similar resilience holon patterns could be compared with each other, identifying best practice in improve resilience situations.

Limitations of the resilience holon include a lack of the following: (i) A scoring system that would enable the resilience holon to be used in a quantitative way, such as to track key performance indicators. (ii) Differentiation between aspects of CES resilience that arise from its architecture, and those that arise during its operational phases. (iii) Analysis of how applicable the resilience holon will be during the design and planning stages of CES, or for resilience situations that are very different from historical ones – such as from an electromagnetic pulse event affecting millions of small electronic devices.

Recommendations for future work include: (i) Testing the applicability of the resilience holon by using it to analyze a wide variety of resilience situations, both historical and predicted. (ii) Developing archetypes of typical resilience situations, represented with the resilience holon, for different types of CES in different situations; this would shorten the time needed to apply it in future. (iii) Developing ways to use the analysis done with the resilience holon to inform quantitative models of CES. (iv) Developing methods for working with groups of stakeholders in applying the resilience holon, similar to group model building [76]; this would enable expert stakeholder knowledge to be incorporated and the narrative of the resilience situation to be communicated visually to others.

Acknowledgment

The authors would sincerely like to thank the seven attendees of an expert workshop, held at Cranfield University, in which an early version of the holon was reviewed and which added significant insights to the study. We also are grateful to the four anonymous reviewers who provided valuable guidance, which led to significant paper improvements. This paper was supported by an early career grant awarded to the corresponding author from ENCORE (the Engineering Complexity Resilience Network, EPSRC grant EP/N010019/1) and by the CECAN (Complexity Methods for Evaluation across the Nexus, ESRC grant ES/S007024/1) and UKCRIC (UK Collaboratorium for Research in Infrastructure and Cities, EPSRC grant EP/R017727/1) grants awarded to the co-author.

References

[1] G. Punzo *et al.*, "Engineering Resilient Complex Systems: The Necessary Shift Toward Complexity Science," *IEEE Syst. J.*, vol. PP, pp. 1–10, 2020, doi: 10.1109/jsyst.2019.2958829.

[2] M. Koshi, "Road Safety - Success and Failure in Japan.," in *13th Australian Road Research Board — 5th Road Engineering Association of Asia and Australasia Combined Conference Proceedings*, 1986, vol. 13, no. 1.

[3] W. Kröger, "Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools," *Reliab. Eng. Syst. Saf.*, vol. 93, no. 12, pp. 1781–1787, 2008, doi: 10.1016/j.ress.2008.03.005.

[4] S. A. Sheard and A. Mostashari, "7.3.1 A Complexity Typology for Systems Engineering," *INCOSE Int. Symp.*, vol. 20, no. 1, pp. 933–945, 2010, doi: 10.1002/j.2334-5837.2010.tb01115.x.

[5] Energy Research Partnership, "Future Resilience of the UK Electricity System," 2018.

[6] M. Bruno, "A Foresight Review of Resilience Engineering: Designing for the Expected and Unexpected. A consultation document," Lloyd's Register Foundation, 2015.

[7] A. Pagano, I. Pluchinotta, R. Giordano, and U. Fratino, "Integrating 'hard' and 'soft' infrastructural resilience assessment for water distribution systems," *Complexity*, vol. 2018, 2018, doi: 10.1155/2018/3074791.

[8] G. C. Gallopín, "Linkages between vulnerability, resilience, and adaptive capacity," *Glob. Environ. Chang.*, vol. 16, no. 3, pp. 293–303, 2006, doi: 10.1016/j.gloenvcha.2006.02.004.

[9] K. Øien, L. Bodsberg, and A. Jovanović, "Resilience assessment of smart critical infrastructures based on indicators," in *Safety and Reliability – Safe Societies in a Changing World. Proceedings of ESREL 2018*, 2018, pp. 1269–1277.

[10] 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, doi: 10.1016/j.ress.2013.07.004.

[11] L. Keller, P. Upadhyaya, and G. Candea, "ConfErr: A tool for assessing resilience to human configuration errors," in *Proceedings of the International Conference on Dependable Systems and Networks*, 2008, pp. 157–166, doi: 10.1109/DSN.2008.4630084.

[12] S. Wang, L. Hong, and X. Chen, "Vulnerability analysis of interdependent infrastructure systems: A methodological framework," *Phys. A Stat. Mech. its Appl.*, vol. 391, no. 11, pp. 3323–3335, 2012, doi: 10.1016/j.physa.2011.12.043.

[13] J. Qin, M. H. Faber, M. Liu, W. Zhang, and D. Lu, "Value of information in resilience management of infrastructure systems," in *IABSE Symposium, Guimaraes 2019: Towards a Resilient Built Environment Risk and Asset Management - Report*, 2019, no. March, pp. 1797–1807.

[14] 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, doi: 10.1016/j.ress.2015.08.006.

[15] F. Ren, T. Zhao, J. Jiao, and Y. Hu, "Resilience Optimization for Complex Engineered Systems Based on the Multi-Dimensional Resilience Concept," *IEEE Access*, vol. 5, pp. 19352–19362, 2017, doi: 10.1109/ACCESS.2017.2755043.

[16] E. Hollnagel, "RAG – Resilience Analysis Grid," in *Resilience engineering in practice. A guidebook.*, Farnham, UK: Ashgate, 2011, pp. 275–296.

[17] S. E. van der Merwe, R. Biggs, and R. Preiser, "A framework for conceptualizing and assessing the resilience of essential services produced by socio-technical systems," *Ecol. Soc.*, vol. 23, no. 2, 2018, doi: 10.5751/ES-09623-230212.

[18] A. Ross and D. Rhodes, "Architecting Systems for Value Robustness and Survivability," in *SysCon 2008 - IEEE International Systems Conference*, 2008.

[19] R. Bhamra, S. Dani, and K. Burnard, "Resilience: The concept, a literature review and future directions," *Int. J. Prod. Res.*, vol. 49, no. 18, pp. 5375–5393, 2011, doi: 10.1080/00207543.2011.563826.

[20] R. Westrum, "A typology of resilience situations," in *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. Woods, and N. Leveson, Eds. CRC Press, 2017.

[21] Y. Y. Haimes, "On the complex definition of risk: A systems-based approach," *Risk Anal.*, vol. 29, no. 12, pp. 1647–1654, 2009, doi: 10.1111/j.1539-6924.2009.01310.x.

[22] United Nations Office for Disaster Risk Reduction, "Report of the open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction," 2016.

[23] International Risk Governance Council, "Governance of Systemic Risks," 2018. [Online]. Available: https://irgc.org/risk-governance/systemic-risks/.

[24] International Risk Governance Council, "Improving the management of emerging risks," 2011.

[25] International Risk Governance Council, "Risk governance. Towards an integrative approach," 2006.

[26] International Risk Governance Council, "Preparing for future catastrophes. Governance principles for slow-developing risks that may have potentially catastrophic consequences.," 2013.

[27] I. Linkov *et al.*, "Changing the resilience paradigm," *Nat. Clim. Chang.*, vol. 4, no. 6, pp. 407–409, 2014, doi: 10.1038/nclimate2227.

[28] R. J. Dawson *et al.*, "UK Climate Change Risk Assessment Evidence

Report: Chapter 4, Infrastructure.," 2016.

[29] IPCC, "Global Warming of 1.5°C. Summary for poicymakers," 2018.

[30] M. Williams, J. Zalasiewicz, P. Haff, C. Schwa gerl, A. D. Barnosky, and E. C. Ellis, "The Anthropocene biosphere," *Anthr. Rev.*, vol. 2, no. 3, pp. 196–219, 2015, doi: 10.1177/2053019615591020.

[31] A. Holdschlag and B. M. W. Ratter, "Multiscale system dynamics of humans and nature in The Bahamas: Perturbation, knowledge, panarchy and resilience," *Sustain. Sci.*, vol. 8, no. 3, pp. 407–421, 2013, doi: 10.1007/s11625-013-0216-6.

[32] A. M. Madni and S. Jackson, "Towards a conceptual framework for resilience engineering," *IEEE Syst. J.*, vol. 3, no. 2, pp. 181–191, 2009, doi: 10.1109/JSYST.2009.2017397.

[33] T. Dolan, "Digitally Connected Infrastructure System Resilience: Literature Review (UCL)," National Infrastrcuture Commission; UCL; Arup, 2017.

[34] P. Greening and C. Rutherford, "Disruptions and supply networks: A multi-level, multi-theoretical relational perspective," *Int. J. Logist. Manag.*, vol. 22, no. 1, pp. 104–126, 2011, doi: 10.1108/09574091111127570.

[35] International Risk Governance Council, "Managing and reducing social vulnerabilities from coupled critical infrastructures," 2006.

[36] A. Koestler, *The ghost in the machine.* Oxford, England: Macmillan, 1968.

[37] S. Valipour, F. Volk, T. Grube, L. Böck, L. Karg, and M. Mühlhäuser, "A formal holon model for operating future energy grids during blackouts," *SMARTGREENS 2016 - Proc. 5th Int. Conf. Smart Cities Green ICT Syst.*, pp. 146–153, 2016, doi: 10.5220/0005768801460153.

[38] H. Paggi and F. Alonso Amo, "Uncertainty and randomness: A holonic approach," in *2010 2nd International Conference on Computer Engineering and Applications, ICCEA 2010*, 2010, pp. 496–503, doi: 10.1109/ICCEA.2010.245.

[39] J. Smuts, *Holism and Evolution*. London: Macmillan, 1926.

[40] E. Tagne Fute and E. Tonye, "Modelling and Self-organizing in Mobile Wireless Sensor Networks: Application to Fire Detection," *Int. J. Appl. Inf. Syst.*, vol. 5, no. 3, pp. 1–7, 2013, doi: 10.5120/ijais12-450874.

[41] E. Negeri, N. Baken, and M. Popov, "Holonic Architecture of the Smart Grid," *Smart Grid Renew. Energy*, vol. 04, no. 02, pp. 202–212, 2013, doi: 10.4236/sgre.2013.42025.

[42] P. Leitão and F. Restivo, "ADACOR: A holonic architecture for agile and adaptive manufacturing control," *Comput. Ind.*, vol. 57, no. 2, pp. 121–130, 2006, doi: 10.1016/j.compind.2005.05.005.

[43] H. Van Brüssel, L. Bongaerts, J. Wyns, P. Valckenaers, and T. Van Ginderachter, "A conceptual framework for holonic manufacturing: Identification of manufacturing holons," *J. Manuf. Syst.*, vol. 18, no. 1, pp. 35–52, 1999, doi: 10.1016/S0278-6125(99)80011-9.

[44] M. Ulieru, "Design for Resilience of Networked Critical Infrastructures," in *2007 Inaugural IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2007)*, 2007, pp. 20–23, doi: 10.1007/978-3-642-40308-8_2.

[45] D. N. Bristow, "Asset system of systems resilience planning: the Toronto case," *Infrastruct. Asset Manag.*, vol. 2, no. 1, pp. 15–22, 2015, doi: 10.1680/iasma.14.00044.

[46] J. W. Hall, J. J. Henriques, A. J. Hickford, and R. J. Nicholls, "Systems-of-systems analysis of national infrastructure," *Proc. Inst. Civ. Eng. Eng. Sustain.*, vol. 166, no. ES5, pp. 249–257, 2013.

[47] M. Jamshidi, *System of Systems Engineering: Innovations for the 21st Century.* New York, NY, USA: Wiley, 2008.

[48] C. Haskins, K. Forsberg, and M. Krueger, "Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities," INCOSE Systems Engineering Handbook v. 3.2.2, 2011.

[49] J. R. Enos, "Achieving resiliency in major defense programs through nonfunctional attributes," *Syst. Eng.*, vol. 22, no. 5, pp. 389–400, 2019, doi: 10.1002/sys.21488.

[50] C. Eckert and O. Isaksson, "Safety Margins and Design Margins: A Differentiation between Interconnected Concepts," *Procedia CIRP*, vol. 60, pp. 267–272, 2017, doi: 10.1016/j.procir.2017.03.140.

[51] M. Heese, W. Kallus, and C. Kolodej, "Assessing behaviour towards organisational resilience in aviation," in *Proceedings 5th Symposium on Resilience Engineering, Managing trade-offs*, 2013, pp. 1–293, doi: 10.1016/j.ssci.2015.02.023.

[52] M. Rahimi and A. M. Madni, "Toward a resilience framework for sustainable engineered systems," *Procedia Comput. Sci.*, vol. 28, no. Cser, pp. 809–817, 2014, doi: 10.1016/j.procs.2014.03.096.

[53] W. R. Ashby, *Introduction to Cybernetics*. London: University Paperbacks, 1964.

[54] C. Nan and G. Sansavini, "A quantitative method for assessing resilience of interdependent infrastructures," *Reliab. Eng. Syst. Saf.*, vol. 157, pp. 35–53, 2017, doi: 10.1016/j.ress.2016.08.013.

[55] M. Thapa, J. Espejo-Uribe, and E. Pournaras, "Measuring network reliability and repairability against cascading failures," *J. Intell. Inf. Syst.*, vol. 52, no. 3, pp. 573–594, 2019, doi: 10.1007/s10844-017-0477-0.

[56] J. Ahern, "From fail-safe to safe-to-fail: Sustainability and resilience in the new urban world," *Landsc. Urban Plan.*, vol. 100, no. 4, pp. 341–343, 2011, doi: 10.1016/j.landurbplan.2011.02.021.

[57] K.-L. Thomson and R. von Solms, "Towards an Information Security Competence Maturity Model," *Computer Fraud and Security*, no. May, pp. 1–10, 2006.

[58] O. L. De Weck, D. Roos, and C. L. Magee, "Engineering Systems - Meeting Human Needs in a Complex Technological World," in *Engineering Systems - Meeting Human Needs in a Complex Technological World*, MIT Press, 2011.

[59] T. Dolan, S. Jude, L. Varga, A. Quinn, and N. Carhart, "Infrastructure resilience: A multi-disciplinary perspective," International Centre for Infrastructure Futures, 2018.

[60] T. Huang, S. L. Voronca, A. A. Purcarea, A. Estebsari, and E. Bompard, "Analysis of chain of events in major historic power outages," *Adv. Electr. Comput. Eng.*, vol. 14, no. 3, pp. 63–70, 2014, doi: 10.4316/AECE.2014.03008.

[61] S. Folga *et al.*, "A systems-level methodology for the analysis of inland waterway infrastructure disruptions," *J. Transp. Secur.*, vol. 2, no. 4, pp. 121–136, 2009, doi: 10.1007/s12198-009-0030-7.

[62] S. Shrivastava, K. Sonpar, and F. Pazzaglia, "Normal accident theory versus high reliability theory: A resolution and call for an open systems view of accidents," *Hum. Relations*, vol. 62, no. 9, pp. 1357–1390, 2009, doi: 10.1177/0018726709339117.

[63] M. Scheffer *et al.*, "Early-warning signals for critical transitions," *Nature*, vol. 461, no. 7260, pp. 53–59, 2009, doi: 10.1038/nature08227.

[64] V. Dakos, E. H. van Nes, P. D'Odorico, and M. Scheffer, "Robustness of variance and autocorrelation as indicators of critical slowing down," *Ecology*, vol. 93, no. 2, pp. 264–271, 2012.

[65] J. Jenkins, T. Nordhaus, and M. Shellenberger, "Energy Emergence: Rebound & Backfire as emergent phenomena," The Breakthrough Institute, 2011.

[66] R. Ramdhany and G. Coulson, "Towards the coexistence of divergent applications on smart city sensing infrastructure," in *CEUR Workshop Proceedings*, 2013.

[67] D. C. Luckham, A. Manens, S. Bhansali, W. Park, and S. Daswani, "Modeling and Causal Event Simulation of Electronic Business Processes," in *ACM Conference on Electronic Commerce EC03*, 2003.

[68] S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, pp. 11–25, 2001.

[69] UKCRIC, Electric Infrastructure Security Council, and ENCORE Network, "The London Black Sky Seminar 2018. Infrastructure and societal resilience to black sky hazards," London, 2018.

[70] M. J. Egan, "Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems," *J. Contingencies Cris. Manag.*, vol. 15, no. 1, pp. 4–17, 2007, doi: 10.1111/j.1468-5973.2007.00500.x.

[71] R. Felix, "A Proposed Taxonomy of Management Systems," *Syst. Res. Behav. Sci.*, vol. 20, no. 1, pp. 21–29, 2003, doi: 10.1002/sres.523.

[72] J. Davis, A. MacDonald, and L. White, "Problem-structuring methods and project management: an example of stakeholder involvement using Hierarchical Process Modelling methodology," *J. Oper. Res. Soc.*, vol. 61, no. 6, pp. 893–904, Apr. 2010, doi: 10.1057/jors.2010.12.

[73] R. Kemp, "Electrical system resilience: a forensic analysis of the blackout in Lancaster, UK," *Proc. Inst. Civ. Eng. - Forensic Eng.*, vol. 170, no. 2, pp. 100–109, 2017, doi: 10.1680/jfoen.16.00030.

[74] R. Kemp, "Living Without Electricity," Royal Academy of Engineering, London, 2016.

[75] Environment Agency, "Estimating the economic costs of the 2015 to 2016 winter floods," 2018.

[76] D. Andersen, J. Vennix, G. Richardson, and E. Rouwette, "Group

Model Building: Problem Structuring, Policy Simulation and Decision Support," *J. Oper. Res. Soc.*, vol. 58, no. 5, pp. 691–694, May 2007, doi: 10.1057/palgrave.jors.2602339.

Rachel Freeman has a BSc. in Mathematics, a MSc. in Renewable Energy and the Environment, and an engineering doctorate in systems from the University of Bristol. She is a research fellow at University College London, working on modelling the complexity of the UK's energy transition towards net zero emissions.

Liz Varga has a BA (Hons) in Pure Mathematics and Data Analysis, a Masters in Business Administration, and a doctorate on aerospace supply chain evolution from Cranfield University. She is professor of complex systems at University College London with a large research portfolio on innovation, resilience and sustainability of infrastructure systems.

[i] A workshop with nine attendees (including the authors) was held at Cranfield University in 2018. Participants had backgrounds in systems engineering (academic and practicing) and ecosystems. The workshop reviewed an initial version of the topic of this paper.

[ii] JustAuto magazine: www.just-auto.com/analysis/thailands-floods-and-their-impact-on-supply-chain-strategies_id127806.aspx

[iii] Hurricane Dorian flooding: https://edition.cnn.com/2019/08/29/us/dorian-path-king-tides-florida-trnd/index.html

[iv] Brownouts in Melbourne: www.abc.net.au/news/2019-01-26/victorian-blackouts-what-caused-them-and-is-this-the-new-normal/10751412