Assessing Resilience in Enterprise Architecture: A Systematic Review

Adina Aldea
Industrial Engineering and Business Information Systems
University of Twente
Enschede, Netherlands
a.i.aldea@utwente.nl

Egle Vaicekauskaitė
Industrial Engineering and Business Information Systems
University of Twente
Enschede, Netherlands
e.vaicekauskaite@student.utwente.nl

Maya Daneva
Services, Cybersecurity & Safety
University of Twente
Enschede, Netherlands
m.daneva@utwente.nl

Jean Paul Sebastian Piest
Industrial Engineering and Business Information Systems
University of Twente
Enschede, Netherlands
j.p.s.piest@utwente.nl

***Abstract*— This review paper aims to explore state-of-the-art research and scientific literature about Enterprise Architecture (EA) resilience. Based on a systematic literature review, 850 articles have been subjected to evaluation for relevance. Based on the findings in 58 selected papers, we conclude that the field of EA resilience is still in its infancy. We identified several definitions and classified six types of resilience measures, based on information type (qualitative/quantitative), the source of the disruption (internal/external), and the duration of the resilience (short-term/long-term). Based on the review, we found 19 metrics that are candidates for EA practitioners to consider for the design of measurement and assessment methods for EA resilience. In addition, we identified relevant research from Information Systems sub-domains and other sciences that can be incorporated to create a holistic view on EA resilience. Based on published definitions of resilience in the selected papers, we propose a definition of the concept of EA resilience. This definition is validated using expert opinion and creates a starting point for reasoning about EA resilience and future research.**

Keywords—resilience, enterprise architecture, systematic review, assessment, metrics, strategy

I. Introduction

During the last decade, many new and complex challenges have arisen due to technological advancements, societal- and environmental changes. The most recent example of such a challenge is the COVID-19 pandemic, which disrupted every aspect of our daily lives and forced us to adapt to completely new and unexpected circumstances. One of the aspects that the COVID-19 pandemic has highlighted over the past few months, is that there is a strong need for system-wide resilience. This design requirement can be realized using Enterprise Architecture (EA). Specifically, the ability of organizations to design resilient EAs and to assess EA resilience is becoming increasingly important for dealing with uncertainty. However, the concept of resilience is widely studied since the seventies, little research and literature is available about EA resilience and the implications. Existing research and literature about EA resilience is scattered; little is known about the possible approaches that organizations and EA practitioners can consider to EA resilience and its related design, measurement, and control. In turn, there is a need to have a more complete understanding of published research on EA resilience to incentivize further discussion. This review paper responds to this need. To our best knowledge and point in time, a systematic review of EA resilience is not performed. Our research goal is to map out (1) the definitions of EA resilience put forward in scientific publications and (2) the published (proposals for) resilience measurement and assessment approaches. Using a Systematic Literature Review (SLR) method [1], we contribute to a better understanding of EA resilience, available research and literature. This review paper provides a starting point for scholars to conduct research about EA resilience and identify future research directions. EA practitioners can benefit from the classified resilience measures and metrics, as a starting point for the design, measurement, and assessment of EA resilience.

This study is structured as follows. Section II presents the background. Section III introduces our research questions and the research process. In Section IV we present the results of the SLR and in Section V we discuss these findings in relation to EA. Section VI contains the results of our first validation with experts and their contributions to theory and practice. The paper concludes in Section VII with the discussion about the findings of this study, the limitations, and recommendations for further research.

II. Background

For the past 40 years, scholars in multiple fields have explored various facets of resilience. The first accepted and best-known definition of 'resilience' stems from the work of Holling (1973) on stability and resilience in ecological systems [2]. Since then, resilience was studied in other domains and disciplines, including engineering, psychology, sociology, and subject to structured literature reviews [3]. Additional systematic reviews are conducted to study resilience both from the perspective of the organization and supply chain [4]. Most recently, Morisse et al. [5] explored Resilience for industry 4.0 manufacturers and reflected on its application? by using the metaphor of building a house. Comprehension of the environment and understanding of an organization's systems forms the foundation of a building. Its main construction relies on four pillars: people, process, technologies, and information. The rooftop of this house is made up of the main characteristics of resilience. This

2325-6362/20/$31.00 ©2020 IEEE
DOI 10.1109/EDOC49727.2020.00011

combined structure forming a house as per [5], results in the resilience of an Industry 4.0 organization.

Based on the current body of knowledge, research, and literature, we can observe that the concept of resilience is studied in multiple domains and disciplines at different aggregation levels. In the field of Information System (IS), the first definition of IS resilience is formulated by Sarkar et al. who also argue that IS resilience falls under Organizational resilience [6]. Given its complex nature, we argue that IS resilience is related to organization resilience but has a much wider scope and application domain. Thus, it should be approached from a multidisciplinary perspective. This motivated us to conduct research about resilience in EA, its position in IS and interconnections with other scientific disciplines and domains.

III. Research Method

A. Systematic Literature Review Method

To structure our research, the well-established Systematic Literature Review (SLR) method of [1] is chosen. Following these guidelines and shown in Fig. 1, our SLR is carried out in three stages: planning, conducting and documentation. The first stage, planning, includes formulating research questions and developing a review protocol. The second stage, conducting, is about performing research: deciding on exclusion and inclusion criteria, relevant databases and performing a search. The third stage, documentation, is a study selection part, where the list of included and excluded studies is created, and the "quality" of primary studies is assessed.

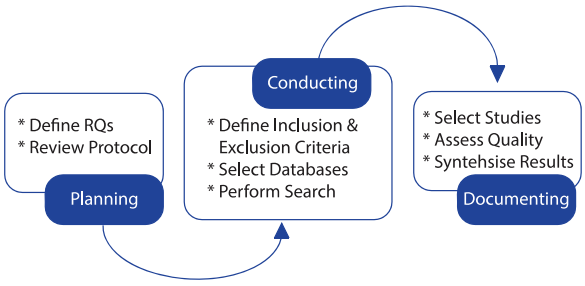

Fig. 1. Process of the Systematic Literature Review.

B. Research Questions

To achieve our research goal stated in the Introduction, we formulated the following Research Questions (RQ):

RQ1: What is the state-of-the-art research on resilience in EA and IS?

RQ2: What are the types of resilience mentioned in scientific literature?

RQ3: What metrics can be used to assess EA resilience, according to scientific literature?

The motivation for RQ1 is to have a deep look at how authors of published research treated the concept of resilience and how they defined it. The motivation for RQ2 is to find what other types of resilience exist in IS sub-areas beyond EA. We believe that several types of resilience could be relevant for EA. The motivation for RQ3 is based on the saying that organizations cannot control what they cannot measure. To understand how resilience can be measured, a comprehensive review of metrics several related domains needs to be performed. We, therefore, are interested to uncover the possible operationalizations of resilience in the context of EA, according to published sources.

C. Our Search Process

We have used the following six scientific databases:

- ACM Digital Library (http://portal.acm.org).
- IEEE Xplore (http://www.ieee.org).
- Science Direct – Elsevier (http://www.elsevier.com).
- Taylor and Francis (http://www.tandfonline.com).
- Scopus (https://www.scopus.com).
- Sage (http://www.sage.com).

As each of the RQs have a different purpose, we have formulated separate queries composed of selected keywords and combinations with the AND/OR logical operators. Each query was focused on retrieving results based on the keywords present in the title, abstract and keywords list of the papers.

RQ1: ("enterprise architecture" OR "Business architecture" OR "information architecture" OR "Technology Architecture" OR "information system") AND resilience.

RQ2: (resilience W/1 [1] type) OR "classification of resilience" OR (resilience W/1 classified) OR (resilience W/1 kind).

RQ3: ("information system*" OR "enterprise architecture" OR enterprise) AND (metric OR measure* OR indicator OR calculation OR formula OR estimat* OR "numerical analysis") AND resilien*.

D. Inclusion and Exclusion Criteria

A set of criteria, as proposed by [1], is defined for selecting the relevant sources. For this study, any paper directly or indirectly discussing resilience is considered to be relevant. To narrow down the results the following inclusion criteria were applied:

- Studies should be in English.
- Articles should be published after 2014 (the first paper on IS resilience is published in 2014).
- Articles should be conference or journal publications (due to more rigorous peer-review process).

E. Study Selection

Numerous results (850 papers) were retrieved from the six databases. To find papers answering our RQs, the retrieved results were sorted out. First, for each RQ, the results were classified in three: Yes, Maybe, No. By reading the title and abstract, it was decided whether a paper is really discussing resilience or just mentioning it as a side topic. If the paper contains important views, it is put to the 'Yes'-labelled folder. If there are doubts about the importance, then it is sorted to 'Maybe'. Finally, if the abstract did not mention any aspect worth looking into the article, the paper is moved to the 'No' folder. When the first phase of sorting to 'Yes', 'No', 'Maybe'

[1] Second keyword needs to appear within 1 word of the first

is finished, the articles in 'Yes' and 'Maybe' folders are evaluated based on full text read. As for the result, irrelevant papers are excluded from the research. The applied selection criteria for the papers are presented below:

1) Does the paper answer the RQs?
2) Is the assessment of resilience the main target?
3) Does the paper contribute to IS or EA?
4) Does the paper provide new insights?

F. Quality Assessment

Following the guidelines of [1], a Quality Assessment was carried out to evaluate collected studies. Thus, four Quality Assessment (QA) questions were treated:

QA1: Was the research question or objective of the paper clearly stated?

QA2: Does a paper contribute to context-independent factors and/or metrics?

QA3: Are the findings based on a realistic case? If not move to Q4.

QA4: For a literature study, is there a comprehensive, systematic approach used in the search strategy?

QA1 its objective is to evaluate whether the studies determine research questions clearly and thoroughly. This contributes to the quality of our review. QA2 checks whether a resilience factor or metric is applicable in a specific context or is context-independent. This division contributes to classifying factors and metrics as part of our review. QA3 is aimed to assess the quality of the paper regarding whether the results are based on a case or not. This will contribute to the utility for EA practitioners. QA4 is to assess the quality of the paper, judging by the structure of the research. This contributes to the comprehension of our review.

G. Data Extraction Form

The data extraction form is designed to present information which is used to address the review questions and study quality criteria. Table I provides an overview of the extracted data, description and relation to our research.

TABLE I. DATA EXTRACTION FORM

No	Extracted data	Description	Type
1	Bibliographic reference	Authors, year of publication, title, and source of Publication	General
2	Type of study	Book, journal article, conference paper, serial, conference proceedings	General
3	Definitions of resilience	Definitions of resilience for Information Systems or Enterprise architecture	RQ1
4	Types of resilience	Definitions of various types of resilience	RQ2
5	Metrics and formulas	Collection of various metrics or formulas for estimating resilience	RQ3

H. Executing the Steps

Table II shows the numbers of papers found per source based on the search queries applied. The initial search performed in April 2020 resulted in 850 papers, of which 72 were selected by following the procedures outlined in the previous sections. Among the results, 13 papers turned out to be duplicated. Thus, the final total number of selected papers is 58.

TABLE II. PAPERS FOUND AND SELECTED PER RQS

Source	RQ1	RQ2	RQ3	Total
ACM Digital Library	7	5	13	25
IEEE	63	13	111	187
Sage	5	19	21	45
Scopus	196	73	56	325
Science Direct	86	-	84	170
Taylor & Francis	48	45	5	98
Total Papers found:	**405**	**155**	**290**	**850**
Total Papers selected:	**24**	**23**	**25**	**58**

IV. RESULTS

In this section, we present the results of the SLR per RQ.

A. Results for RQ1

Based on the selected papers for RQ1, we were able to classify the information retrieved into four groups: definition, strategy, characteristics, and phases as shown in Table III.

TABLE III. RESULTS FOR RQ1

Topic	Findings	Sources
Definition	IS resilience is the ability of a system to work under predicted or unforeseen disruptions and to return to equilibrium or recover to an acceptable level of performance as soon as possible. It aims to mitigate the likelihood of failures and losses and requires constant adaptation to new known or unknown threats	15 papers [7-21]
Characteristics	Diversity, efficiency, adaptability, cohesion, self-organisation, robustness, learning, redundancy, rapidity, flexibility, equality, agility, vulnerability to risk, responsiveness	7 papers [9, 13, 18, 22-25]
Strategy	The strategy of IS resilience should be aligned with organisational resilience and aiming to provide solutions which would be independent of a specific scenario or event. It should also provide alignment between IT and business strategies	2 papers [9, 26]
Phases	Avoidance (Resistance), Absorptive, Adaptive, Recovery (Restorative)	13 papers [8, 9, 11, 13, 18, 20-25, 27-29]

Within the papers selected for answering RQ1, no concrete definition for EA resilience is provided (i.e. defining which strategies would be most appropriate, which characteristics would be most relevant or how the phases of resilience would be applied). While all the selected papers included a generic definition of resilience, only three defined IS resilience [9, 11, 14]. Furthermore, the topic of strategies for IS resilience is barely covered by the selected publications, with only one [26] mentioning actual strategies that could be used. Finally, the characteristics and phases of resilience are covered by several papers, indicating some maturity of the research on the definitional aspects of resilience.

B. Results for RQ2

When analyzing the results for RQ2, we found that there is a growing body of literature concerning the different types of resilience. Two of the most studied forms of resilience are engineering and ecological, as indicated by [30]. Nonetheless, the studies that resulted from the SLRs mentioned in the

background section cover many more domains which have emerged over time. Table IV presents the search results of our SLR. Therein, next to the application domain, we classified the selected papers based on the type of resilience measures (qualitative/quantitative), the source of the disruption (internal/external), and the duration of the resilience measures (short-term/long-term). However, most papers did not provide information that could be used to classify them beyond the application domain.

TABLE IV. RESULTS FOR RQ2

Domain	Qualitative	Quantitative	External	Internal	Short-term	Sources
Community						[23, 31-33]
Critical Infrastructure						[17, 23, 34]
Cyber						[35-37]
Ecological	X				X	[33, 38-40]
Economic			X	X		[23, 29, 40-42]
Engineering		X			X	[23, 33, 38, 40, 43]
Organisation	X		X	X		[5, 7, 9, 17, 21, 23, 29, 33, 38, 42, 44-46]
Social			X			[23, 24, 29]
Social-ecological					X	[40, 47]
System	X					[23, 45]
Technical			X	X		[17, 29, 42]
Urban						[33, 48]
Total	**3**	**1**	**4**	**3**	**3**	

From the selected papers for answering RQ2, only three discuss resilience from the perspective of the source of disruption [23, 29, 34]. External disruptions can be caused by government, society, or other external stakeholders, while internal disruptions can come from the critical infrastructure within an organization [34].

Similarly, we found only two papers discussing the duration of resilience. [49] state that short-term resilience refers to the restoration of regular services and financial activities after being confronted with short-term disturbances. Another perspective comes from [50], who argue that short-term resilience is the ability to cope with altering conditions or a capacity to reduce the consequences of disruption. Long-term resilience is described as constantly evolving and changing and providing a response to a range of long-term stressor [49]. [50] present a framework for long-term resilience in their paper which consists of a cycle of 4 functions and 4 different states. However, since none of the selected papers relates long-term resilience to a domain of application, this property is removed from Table IV.

C. Results for RQ3

The results for RQ3, as shown in Table V, provide an overview of the types of metrics suitable for assessing resilience and the ways these metrics are calculated.

We found that most of the metrics identified from the selected papers can be expressed quantitatively, with the help of mathematical formulas, except for Collaboration, Connectivity, Diversity, Flexibility, Knowledge sharing, and Redundancy. Additional measures and ratios can be developed to some extent. As also indicated in Table IV, all the quantitative metrics come from the Engineering domain. The quantitative metrics which are mostly mentioned in the selected papers are Recovery time [12, 51, 52] and Performance loss [51-53]. This finding is not surprising as one of the foci in engineering resilience is to minimize the values of these two metrics.

TABLE V. RESULTS FOR RQ3

Metric	Definition	Source
Capability Drop Ratio	Capability degradation by the influence of disturbances	[54]
Capability Recovery Degree	Margin of recovery when capability restores from the lowest level to a new dynamic steady state	[54]
Capability Recovery Ratio	Percentage of capability restored after the influence of disturbances	[54]
Collaboration	Ability to work together and share knowledge within the organization	[5]
Connectivity	Connections on all levels, from process to product	[5]
Degrading time	Time that it takes for a system to reach its bottom in case of attack	[52]
Diversity	Option to choose from a variety of different assets, institutions, etc.	[5, 13, 55]
Flexibility	Systems property to change to new status easily	[5, 13, 56, 57]
Knowledge sharing	Ability to reach and share common knowledge effectively among members	[5, 13, 56]
Performance degradation	Maximal performance degradation due to incident	[52, 54]
Performance loss	Indicates system performance degradation during the transients of a disruptive event	[51-53]
Production loss	Production loss caused by disruption, during and after the disruption	[12]
Protection time	Time that a system managed to absorb incident	[52]
Recovery time	Time that a system takes to recover after the disruption	[12, 51, 52]
Redundancy	Extent to which components within a system are substitutable	[13]
Robustness	Amount of time to recover to an acceptable level of functionality	[13, 53]
Total loss	Total financial loss experienced by an organization due to disruption	[52]
Total time underproducing	Total time when system production rate was lower than its steady-state	[12, 51]
Vulnerability	Probability of occurrence of unforeseen disruptions	[58]

When analyzing the results for RQ3, we noted that several metrics have multiple names based on the papers that they are retrieved from. For example, ‘robustness’ and ‘rapidity’ both signify how quickly a system recovers to the first degree of functionality. Similarly, ‘flexibility’ and ‘adaptability’ are both used to measure the ability of a system to change status [5, 13, 56].

V. DISCUSSION

This SLR revealed that resilience has been increasingly recognised as an indispensable property in various domains. Thus, it was expected that resilience in the IS domain would be explored more in-depth than what is currently provided in the literature. Similarly, papers discussing EA resilience are scarce and research is in its infancy.

Of the selected 58 papers, most of them (39 papers) are published in journals which indicates a certain level of maturity of IS resilience research. However, this could also be explained by the fact that IS resilience research is based on

two mature fields (IS and resilience). Furthermore, most of the selected papers (32% representing 18 papers) were published in 2016 which is a few years after the first publication on IS resilience (2014). This skewness in the results could be related to the search query that we used which focuses on more fundamental research, such as definitions, strategies, and types of resilience. These papers are mostly found until 2016. The papers that are published after 2016 seem to have a focus on defining metrics and the characteristics of resilience. Finally, while most of the selected papers are published by authors from the USA (30% representing 31 authors), the spread of authors covers 30 different countries. Thus, it can be said that while the USA has a stronger presence in IS resilience research, but it is by no means the only one, as countries such as Portugal, UK and Australia each represent 15% of authors.

A. Definition of Resilience

When analyzing the papers discussing IS resilience, we encountered a controversial topic, namely whether IS resilience is part of Organizational resilience or vice-versa. Organizational resilience is a more mature domain which is identified as a means to work reliably in many different adverse situations while IS resilience is more focused on providing secure and dependable systems. Thus, it can be considered that Organizational resilience is a broader field and it is understood that when a disturbance happens in an IS, it affects the whole organization. Therefore, it can be considered that IS resilience is part of Organizational resilience. On the other hand, as organizations are increasingly dependent on their supply chain partners and corresponding networks, platforms, and ecosystems, one could argue that IS resilience can be positioned next to Organizational resilience.

Of all the selected papers, only [9] provides a concrete definition of IS resilience, namely: IS resilience is the management of IS "vulnerabilities, and adaptive capacity, risk intelligence, flexibility and agility of IS in a complex, dynamic, and interconnected environment." Multiple resilience characteristics are covered by this definition: system awareness, vulnerability, adaptability, flexibility, and agility. Also, the link is made to a larger system and the dynamics and complexity of the environment. A slightly different approach is taken by [11] where the focus is on the four phases of IS resilience: "the capacity to prepare and adapt facing perpetuating evolutionary conditions and to restore full capability after an accident or an attack." [14] outlines that systems should recover, rebound or jump back to the primary or addressed system state. [13] argues that most research focuses on the restorative phase of resilience which the adaptive phase is still understudied. Taken together, one can study IS resilience in a narrow sense on system-level, study the resilience of systems in the context of a wider system or network and chose to focus on specific phase or develop an integrative view.

To define EA resilience, we first need to consider what EA is. According to [30], EA provides a common view on how the enterprise resources (product, process, technology, information and application architecture) are integrated and associated to each other to provide the primary drivers of the enterprise. Thus, based on the selected papers and the definition of EA, we can draw the following conclusions about EA resilience. Namely, that is has a broader focus than the definition of IS resilience, by including several aspects such as stakeholders, goals, processes and functions, applications and data, products and services, technology, and physical elements. Thus, it covers elements of both IS and Organisational resilience and is part of a larger system and environment. Furthermore, the effects of the disruption are shown on the integrated architecture of an organisation and not only based on the relations between systems. As a result, we could define *EA resilience as the ability of an organisation to identify and assess the vulnerabilities of enterprise resources in its integrated architecture and prepare for disruptions, by designing specific measures in an EA to increase its capabilities to adapt to new or changing circumstances and restore full capability after an unexpected disruption.*

B. Types of Resilience

From the selected papers we could identify that resilience is studied in relation to several domains which can provide insights for IS and EA resilience. Amongst these are the domain of Engineering which has well-established research on quantitative metrics that can be used to assess resilience, and the domain of Organisational resilience which provides insights into having a strategic perspective on threat assessment and knowledge sharing. Other notable domains are Critical infrastructure (systems, networks and assets), System (system performance), Technical (technical infrastructure) and Cyber resilience (the process of ensuring the protection of core functionality and defining straightforward ways to restore and lower priority functions).

Of these aforementioned domains, Cyber resilience is an obvious choice to consider as part of IS and EA resilience. [35] propose the following seven steps for ensuring cyber resilience, which could also be applied to EA resilience:

1) Classification – classifying threats.

2) Risk assessment – providing a detail description of every threat and the possible harm.

3) Ranking – all threats are ranked thus it would be assured that assets ranked as "critical" would be maintained and assigned to supervise.

4) Design and deployment – identify controls objectives, design an infrastructure to ensure its stated mission, goals and objectives and deploys it.

5) Test – checking the critical control performance against stated mission goals.

6) Recovery – a creation of a complete and consistent recovery process.

7) Evolvement – deploying process and technology improvements.

Regarding the duration of resilience, none of the selected papers discussed long-term resilience in relation to any application domains. However, since the duration mostly depends on the strategy employed and the circumstances of the disturbance, it can be said that long-term resilience is relevant for all application domains.

One of the most controversial aspects we discovered from the selected literature was that disruptions such as pandemics are categorised under short-term resilience [49]. Considering the current COVID-19 pandemic and that short-term resilience is about recovering quickly, this classification might change. The current pandemic is having a prolonged global impact on all levels of our society and thus could be classified as long-term.

C. Characteristics of Resilience

IS resilience as a property can be seen from three different perspectives: resilience as a property of the IS input system, resilience as a property of the IS itself and resilience as a property of the IS output system [13]. Various characteristics are mentioned in multiple papers, including diversity, efficiency, adaptability, cohesion, self-organisation, robustness, learning, redundancy, rapidity, flexibility, equality, agility, vulnerability to risk, responsiveness. People, organisations, and communities also have an impact on IS resilience, because it involves use, impact and effects. Besides the adaptability of systems, it is also expected that the personnel is flexible, motivated, optimistic and consistent [22], which also makes it sensitive to cultural aspects and biases.

From an EA perspective, it could be argued that all of the characteristics of IS resilience are also relevant for EA resilience. For example, a characteristic such as Redundancy can be reflected in an EA model as a secondary Application component or Node which are performing the same task and can be used interchangeably (e.g.: a backup database in the cloud for all the company data). However, assessing Redundancy from a broad perspective might lead to different resilience measures (e.g. supply chain partners have different backup procedures) and additional issues (e.g. network latency). Another example is Diversity, which could be reflected in an EA model as Application components or System software that are provided by different partners. Characteristics such as Self-organisation, Adaptability, Flexibility and Agility are more difficult to express since there is no direct way to model them and measure them to be system-specific or context-dependent.

D. Strategies for Resilience

In the selected literature, the concept of 'Strategy' is linked to the understanding of a disaster. Following the proposed lifetime of a disaster, three phases can be identified: readiness, responsiveness, and recovery. Various strategies can be applied to each of the phases to reach better results. The readiness phase takes place while the planned level of operations is maintained. Several strategies are proposed for this stage. Inventory control and safety stocks, investing in training and education, learning from the experience of others, predicting the likelihood of event and warning, identifying threats, and building common knowledge also play a role. The second phase is the Response to a disaster. The system enters this phase when it failed in the first phase and the disturbance occurred. During this phase, the system has one aim, namely, to withstand, absorb the impact and keep the performance as high as possible. At this point, strategies which include risk-hedging and information sharing, using the plans created during the stage of readiness, and reorganising resources, are commonly used. The third phase is Recovery. It starts when the disturbance has subsided and finishes when the system is back to a pre-disruption or normal operational state. At this stage repairing, restoring and rebuilding tasks are performed, identifying learned lessons and best practices. [25] presents a list of various strategies which could be applied during different phases (Table VI).

TABLE VI. RESILIENCE STRATEGIES FOR DIFFERENT PHASES.

Strategy	Readiness	Response	Recovery
Acceptance		X	
Barbell	X		
Buffering	X		
Collaboration	X	X	X
Cost Minimization	X		
Customer Service			X
Creating Disruption Management Culture	X		
Crisis Management	X	X	X
Demand Managing		X	
Forecasting	X		
Fault Injection	X		
Government Lobbying		X	
Graceful Degradation		X	
Insurance	X		
Infrastructure Investments	X		
Inventory Management	X		
Knowledge Management			X
Mapping	X		
Network Structure Planning	X		X
Postponement		X	
Performance measurement			X
Policy management	X	X	
Real-time monitoring	X		
Reengineering	X		
Risk Assessment	X		
Risk-hedging	X		
Revision		X	X
Sensemaking		X	X
System Analysis/Evaluation	X		
Supplier Selection	X		
Sourcing	X	X	
Weak links		X	

As mentioned before, IS resilience falls under Organisational resilience, thus both strategies should be aligned with each other [8]. Business has an important role in IS too. Thus, four relevant aspects of planning are distinguished: IT and business strategies should be aligned, IT investment in strategic priorities should receive more attention, discussions on ways to avoid potential business risks should be held and capitalization on current business opportunities should be considered [8]. According to [59], the following four parts of a strategy can be outlined:

1) Structured evaluation and exploration of disruption risks as well as a continued search of possible improvements for warning systems and general awareness of the underlying causes.

2) Raising awareness of responsibilities.

3) Long-term strategies and preventive measures.

4) Cooperation with partners on advanced planning and quick response, assessments of risk factors.

When considering which of the strategies would be suitable for EA resilience, several stand out. For example, a Risk assessment strategy is in line with the current scientific

literature on EA [60] and with the practitioner-focused approach, e.g. described in papers from the Open Group [61]. Similarly, a re-engineering strategy matches the purpose of EA which is to help organisations with designing and re-designing resilience in their architecture to fit the organisational goals and strategies. Other suitable strategies for EA would be Cost minimisation and Performance measurement which align with literature that proposes Cost and Performance analyses for EAs [62].

E. Phases of Resilience

The four phases of resilience identified in Table III, Avoidance, Absorptive, Adaptive and Recovery, are considered as a sequence for reacting to disturbances. When a disturbance occurs, the first thing a resilient system should be able to do is to withstand the situation without any consequences and avoid negative impact. If a system is not capable of this, the absorption phase is started where the system performance is not capable to keep up with disruption and starts decreasing. At this stage, the system might need to adapt to continue a certain level of performance, by adjusting its process or requiring maintenance if it is a technical issue, etc. If the system performance drops to zero, the resilience process stops. If the system can maintain some level of performance, it moves to the last phase, namely recovery.

The four phases of resilience we identified can also be related to the three strategies for addressing resilience. Namely, a resilient system has a chance of Avoiding disturbances without interference to its performance only if certain Readiness strategies are employed by an organisation. Similarly, the ability of a system to Absorb and Adapt to a disturbance depends on the kinds of Response strategies of the organisation. If the Response strategies are not adequate, then the disruption cannot be handled by the system and its performance will drop to zero. If the strategies are effective and the system can maintain some adequate performance levels until the disruption subsides, then the Recovery strategies can be employed in the Recovery phase.

From the perspective of EA, all four phases of IS resilience are applicable. The EA of an organisation should be resilient by design, which implies that many disturbances should be avoided due to the configuration of the architecture. For disturbances that are not avoidable, the EA should have the ability to absorb (part of) the shock while maintaining at the business processes operational. If this is not possible, then the application and technology architectures need to be adjusted to support at least the critical business processes that help achieve the most important organisational goals. Once the intensity of the disruption decreases, the processes of the organisation can slowly return to normal while the performance of the EA should reach an equilibrium. For Enterprise Architects to be able to estimate the resilience of their EA, the three aspects should be estimated (based on the definition of engineering resilience): the entity of changes and disruptions, the optimal performance and its deviation, and the expenses due to adjustments [20].

F. Metrics of Resilience

Based on the SLR we identified 19 metrics (Table V), most of which are quantitative and come from the Engineering domain. Some of the identified metrics are also relevant for assessing EA resilience. For example, Vulnerability is the property defining how easily a system can be exposed to risk and cause disturbances. It is closely related to the ability to learn, anticipate, and monitor. The extent and duration of the disruption are calculated by the product of the probability of the disruption occurring and the level of its consequences which determine the vulnerability to risk. this type of risk calculation has also been proposed by the Open Group [61]. Other examples of applicable metrics are Redundancy (the extent to which components within a system are substitutable), Diversity (variety in assets, equipment, systems, etc. used), Performance loss (degradation during the occurrence of a disruptive event), Total loss (total financial loss experienced by the organisation due to the disruption).

VI. First Validation and Reflection on the EA Resilience Definition

Our first validation of the proposed definition was to collect and analyzed feedback of experts in EA. For this expert-based evaluation [63], we employed qualitative perception-based evaluation techniques. Given the intended audience of our research, we consulted 2 experienced EA researchers (RES) and 2 EA practitioners (PRA) for their expert opinions on our definition. The collection of our experts' opinions is conducted by using a form with questions, in which the respondents directly write their answers. Our feedback form contains a section for general comments in regard to the definition, specific feedback in regard the logic and arguments, its value for theory and value for practice, and any other comments or questions. In addition, the feedback form contains questions about the profile of the consulted experts. Table VII summarizes the background and experience of our four experts. Therein, 'n/a' stands for 'not applicable'.

TABLE VII. Background and Experience of Consulted Experts

Profile	**RES1**	**RES2**	**PRA1**	**PRA2**
Education level	PhD	MSc	MSc	MSc
Current profession	Professor	PhD candidate	Enterprise Architect	Independent EA Consultant
Years of experience (in years)				
EA research	18	2	n/a	n/a
EA education	16	6	n/a	10
EA implementation/ consulting	7	2	21	10
Knowledge/confidence in assessing and modelling of (1-5 scale [a]):				
Value concepts	5	2	4	5
Risk and security concepts	5	3	5	5
Resilience concepts	5	4	4	3

[a] 1-5: none, low, medium, high, expert.

In what follows, we first present the findings of our first validation together with our reflection on the results, followed by a discussion on the contributions to theory and practice.

A. Expert Opinions and Refection on the Results

RES1 suggests improving the balance of researchers' and practitioners' perspectives by shortening the definition. While it might be suitable for academic purposes, it could be easier to use for practitioners if the first half would be dropped. A slightly differing opinion comes from RES2 who considers that the definition might not include all relevant

aspects. They suggest considering the anticipation of disrupting behavior and the acknowledgement of sources which are detrimental for emergent behaviors which are neither predictable nor intended by design. We consider that while the definition could be made shorter by removing certain parts, it would not reflect the complete meaning of what we envision it should be based on the literature review. Additionally, in further research, another review should be performed to explore the aspects of emergent behavior to establish its relation to our EA definition.

Furthermore, RES1 considers that the definition should be extended to reflect Enterprise resilience and not just EA resilience to better reflect the overall purpose of resilience. This aligns with the opinion of PRA2 who suggests adding an extra dimension to the definition focusing on the interaction of actors within an organization in changing circumstances which require adaptation. Lastly, PRA1 mentions that the definition aligns with the topics of cybersecurity, crisis management and business continuity, which are considered important for EA resilience. We agree that the scope of the definition might need to be extended to incorporate additional perspectives and fields of study. Thus, future research should be conducted to see how this definition can be extended while maintaining its original purpose.

Regarding the terminology used in the definition, RES2 suggests removing the word "full" in relation to the restoring of the capabilities of an architecture after a disruption. Although restoring full capability may be desirable, this may not always be feasible and realistic to achieve. Thus, terms such as "acceptable" or "anticipated" would be preferred. Furthermore, RES2 advises removing the term "unexpected" as this suggests that the EA resilience should only focus on unexpected events, whereas certain events can also be expected and incorporated in the design of the architecture. Moreover, PRA1 suggests changing the term "circumstance" to "context" to make the definition more suitable. We consider that these suggested changes would be beneficial for the definition as they bring it closer to its purpose.

B. *Contributions to Theory and Practice*

Our experts indicated some implications of our definition for practice. First, the two practitioners agreed that they could work with the definition, which gives us a hint that EA practitioners might find it useful in their projects. Of course, more research is needed in more organizations, to substantiate this claim. Second, PRA 2 remarked that the reasoning about resilience should strike a balance between local and integral thinking. According to this practitioner, local thinking is about the support of capabilities and resources (incl. people and technology), while integral thinking is about synchronization and coordination (priorities, compliance, standards, policy). Our definition fits best at a central level. This allows us to think that our definition might be considered most suitable for use to architects operating at this level. This, of course, is a working hypothesis, which could be studied empirically in further research.

Our definition also has some implications for theory. Following Wieringa [64], for researchers to reason be able to reason about a newly emerging scientific sub-field, they need a set of concepts and relationships describing aspects of the phenomena of interest in this sub-field. Our SLR is a step in this direction. Using concepts aggregated from literature sources, we proposed a definition which states what authors of published research deemed important theoretical concepts in their published works. We consider this definition to be only the beginning of an ongoing conversation on EA resilience in the EA community. We expect the definition to evolve as more empirical studies in organizations get published and new evidence is produced. As a definition is used, its qualities and possible needs for revisions will become clearer. For example, how our definition relates to sub-fields such as business continuity and crisis management? How it relates to EA investment decision-making? Empirical follow-up work could answer these interesting questions and therefore forms a line for future research.

VII. Conclusion

This paper reported results from a SLR that provided an overview of the current state-of-the-art research and literature on resilience in the field of EA and IS. Our initial goal was to focus exclusively on EA literature, however, due to a limited number of papers of this topic, we extended our scope to cover the broader field of IS.

A. *Summary of findings and results*

The contribution of this SLR is as follows: First, it discusses the definition of IS resilience. Second, it identifies several suitable strategies, characteristics, phases and measurements of IS resilience. Third, we position IS resilience next to organizational resilience and incorporate concepts from other disciplines and domains. Fourth, based on our findings, we have presented our view of how these could be applied and related to EA, starting with providing our definition for EA resilience. Furthermore, we have categorized 6 different resilience types based on their domain of application, the duration of the resilience (short-term/long-term), the types of measures (quantitative/qualitative) and the source of the disruption (internal/external). Moreover, we have provided an overview of relevant metrics (Table V) which could be used for assessing IS resilience. Based on this, we have proposed several metrics that could be applied to assess EA resilience as well. Taken together, our work provides a starting point for structured reasoning about EA resilience and future research.

B. *Limitations and Further Research*

One of the main limitations of our research is that with the limited research currently available on EA resilience we have chosen to expand the scope and focus on IS resilience instead. While many of the aspects that are relevant for IS resilience are also applicable for EA, during this study we could only provide our suggestions for what these might be. Thus, the focus of our research is on a sub-domain and we suggest that further research should try to identify which of the 19 metrics (Table V) can be used to assess EA resilience and how this can be done.

Furthermore, from our experience with EA modelling, we can conclude that most current models are not expressive enough for supporting all types of resilience assessment. Thus, we suggest future work should be done in designing

architectural patterns which correspond with certain characteristics of resilience. One such example could be to use OR-junctions to signify when two elements of an EA are interchangeable. This would facilitate the assessment of EA redundancy. Existing structured approaches, such as TOGAF, can be used as a starting point to explore and develop practical approaches for EA practitioners.

Moreover, our focus on the IS field limited our ability to uncover research from other domains (as identified in Table IV). This means that potentially relevant research for EA resilience was not included in our sample. Thus, we suggest that further research should focus on including information from additional domains of application (e.g., Cyber, Critical infrastructure, Engineering, Organizational, System, Technical) to have a more comprehensive input for defining all aspects of EA resilience. Furthermore, an emphasis should be placed on exploring literature beyond the IT aspects of enterprise resilience and incorporate knowledge from areas such as Social Sciences, Logistics, Manufacturing, and other external environment perspectives. This would allow to provide a comprehensive view on Enterprise Architecture resilience.

ACKNOWLEDGMENT

The authors thank the anonymous reviewers for their constructive feedback. A special word of thanks is for our experts who have helped us with our first validation of the EA resilience definition.

REFERENCES

[1] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele University, 2007. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.471&rep=rep1&type=pdf

[2] C. S. Holling, "Resilience and Stability of Ecological Systems," *Annual Review of Ecology and Systematics,* vol. 4, no. 1, pp. 1-23, 1973, doi: 10.1146/annurev.es.04.110173.000245.

[3] R. Bhamra, S. Dani, and K. Burnard, "Resilience: The concept, a literature review and future directions," *International Journal of Production Research,* Review vol. 49, no. 18, pp. 5375-5393, 2011, doi: 10.1080/00207543.2011.563826.

[4] M. Kamalahmadi and M. M. Parast, "A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research," *International Journal of Production Economics,* Article vol. 171, pp. 116-133, 2016, doi: 10.1016/j.ijpe.2015.10.023.

[5] M. Morisse and C. Prigge, "Design of a business resilience model for industry 4.0 manufacturers," in *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation*, 2017, vol. 2017-August.

[6] A. Sarkar, S. Wingreen, and J. Ascroft, "Governing information systems resilience: A case study," 2016: University of Piraeus.

[7] A. Amaral, G. Fernandes, and J. Varajão, "Identifying Useful Actions to Improve Team Resilience in Information Systems Projects," in *Procedia Computer Science*, 2015, vol. 64, pp. 1182-1189, doi: 10.1016/j.procs.2015.08.549.

[8] A. Sarkar, S. Wingreen, and J. Ascroft, "Governing information systems resilience: A case study," in *Proceedings of the 13th European, Mediterranean and Middle Eastern Conference on Information Systems, EMCIS 2016*, 2016, pp. 320-331.

[9] A. Sarkar, S. Wingreen, and J. Ascroft, "Top management team decision priorities to drive IS resilience: Lessons from Jade Software Corporation," in *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*, 2016.

[10] R. K. Buchanan, S. R. Goerger, C. H. Rinaudo, G. Parnell, A. Ross, and V. Sitterle, "Resilience in engineered resilient systems," *Journal of Defense Modeling and Simulation,* Article in Press 2018, doi: 10.1177/1548512918777901.

[11] W. Goudalo and C. Kolski, "Towards advanced enterprise information systems engineering: Solving resilience, security and usability issues within the paradigms of socio-technical systems," in *ICEIS 2016 - Proceedings of the 18th International Conference on Enterprise Information Systems*, 2016, vol. 2, pp. 400-411, doi: 10.5220/0005835904000411.

[12] X. Gu, X. Jin, J. Ni, and Y. Koren, "Manufacturing system design for resilience," in *Procedia CIRP*, 2015, vol. 36, pp. 135-140, doi: 10.1016/j.procir.2015.02.075.

[13] R. Heeks and A. V. Ospina, "Conceptualising the link between information systems and resilience: A developing country field study," *Information Systems Journal,* Article vol. 29, no. 1, pp. 70-96, 2019, doi: 10.1111/isj.12177.

[14] R. Pirinen, "Towards common information systems maturity validation Resilience Readiness Levels (ResRL)," in *IC3K 2017 - Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, 2017, vol. 3, pp. 259-266, doi: 10.5220/0006450802590266.

[15] M. Sakurai, R. T. Watson, and J. Kokuryo, "How do organizational processes recover following a disaster? A capital resiliency model for disaster preparedness," 2016: IEEE, pp. 2862-2871.

[16] R. Almeida, A. A. Neto, and H. Madeira, "Resilience benchmarking of transactional systems: Experimental study of alternative metrics," in *Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC*, 2017, pp. 40-49, doi: 10.1109/PRDC.2017.15.

[17] D. Rehak, P. Senovsky, M. Hromada, and T. Lovecek, "Complex approach to assessing resilience of critical infrastructure elements," *International Journal of Critical Infrastructure Protection,* Article vol. 25, pp. 125-138, 2019, doi: 10.1016/j.ijcip.2019.03.003.

[18] S. Slivkova, D. Rehak, V. Nesporova, and M. Dopaterova, "Correlation of Core Areas Determining the Resilience of Critical Infrastructure," in *Procedia Engineering*, 2017, vol. 192, pp. 812-817, doi: 10.1016/j.proeng.2017.06.140.

[19] W. Urbanczyk and J. Werewka. *Enterprise architecture approach to resilience of government data centre infrastructure, Advances in Intelligent Systems and Computing*, vol. 852, pp. 135-145, 2019.

[20] A. Pasquini, M. Ragosta, I. A. Herrera, and A. Vennesland, "Towards a measure of Resilience," in *Proceedings of ATACCS 2015 - 5th International Conference on Application and Theory of Automation in Command and Control Systems*, 2015, pp. 121-128, doi: 10.1145/2899361.2899374.

[21] S. R. Velu, A. Al Mamun, T. Kanesan, N. Hayat, and S. Gopinathan, "Effect of information system artifacts on organizational resilience: A study among Malaysian SMEs," *Sustainability (Switzerland),* Article vol. 11, no. 11, 2019, Art no. 3177, doi: 10.3390/su11113177.

[22] B. Barn and R. Barn, "Resilience and values: Antecedents for effective co-design of information systems," in *23rd European Conference on Information Systems, ECIS 2015*, 2015, vol. 2015-May.

[23] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliability Engineering & System Safety,* vol. 145, pp. 47-61, 2016.

[24] S. Platt, D. Brown, and M. Hughes, "Measuring resilience and recovery," *International Journal of Disaster Risk Reduction,* vol. 19, pp. 447-460, 2016.

[25] J. Ramezani and L. M. Camarinha-Matos, "Approaches for resilience and antifragility in collaborative business ecosystems," *Technological Forecasting and Social Change,* vol. 151, p. 119846, 2020.

[26] A. Marrella, M. Mecella, B. Pernici, and P. Plebani, "A design-time data-centric maturity model for assessing resilience in multi-party business processes," *Information Systems,* vol. 86, pp. 62-78, 2019.

[27] S. Hosseini, A. Al Khaled, and M. D. Sarder, "A general framework for assessing system resilience using Bayesian networks: A case study of sulfuric acid manufacturer," *Journal of Manufacturing Systems,* vol. 41, pp. 211-227, 2016.

[28] H. Elleuch, E. Dafaoui, A. El Mhamedi, and H. Chabchoub, "A quality function deployment approach for production resilience improvement in supply chain: case of agrifood industry," *IFAC-PapersOnLine,* vol. 49, no. 31, pp. 125-130, 2016.

[29] L. Labaka, J. Hernantes, and J. M. Sarriegi, "Resilience framework for critical infrastructures: An empirical study in a nuclear plant," *Reliability Engineering & System Safety,* vol. 141, pp. 92-105, 2015.

[30] R. Gomes, "Resilience and enterprise architecture in SMES," *JISTEM-Journal of Information Systems and Technology Management,* vol. 12, no. 3, pp. 525-540, 2015.

[31] T. Comes, "Designing for networked community resilience," *Procedia engineering,* vol. 159, pp. 6-11, 2016.

[32] A. Ostadtaghizadeh, A. Ardalan, D. Paton, H. Jabbari, and H. R. Khankeh, "Community disaster resilience: A systematic review on assessment models and tools," *PLoS currents,* vol. 7, 2015.

[33] J. Van Trijp, K. Boersma, and P. Groenewegen, "Resilience from the real world towards specific organisational resilience in emergency response organisations," *International journal of emergency management,* vol. 14, no. 4, pp. 303-321, 2018.

[34] L. Labaka, J. Hernantes, and J. M. Sarriegi, "A holistic framework for building critical infrastructure resilience," *Technological Forecasting and Social Change,* vol. 103, pp. 21-33, 2016.

[35] W. A. Conklin and D. Shoemaker, "Cyber-resilience: Seven steps for institutional survival," *EDPACS,* Article vol. 55, no. 2, pp. 14-22, 2017, doi: 10.1080/07366981.2017.1289026.

[36] J. Hua, Y. Chen, and X. R. Luo, "Are we ready for cyberterrorist attacks?—Examining the role of individual resilience," *Information & Management,* vol. 55, no. 7, pp. 928-938, 2018.

[37] R. F. Babiceanu and R. Seker, "Trustworthiness requirements for manufacturing cyber-physical systems," *Procedia Manufacturing,* vol. 11, pp. 973-981, 2017.

[38] J. L. Davidson *et al.*, "Interrogating resilience: toward a typology to improve its operationalization," *Ecology and Society,* vol. 21, no. 2, 2016.

[39] S. Rocchetta and A. Mina, "Technological coherence and the adaptive resilience of regional economies," *Regional Studies,* vol. 53, no. 10, pp. 1421-1434, 2019.

[40] M. Sabatino, "Economic crisis and resilience: Resilient capacity and competitiveness of the enterprises," *Journal of Business Research,* vol. 69, no. 5, pp. 1924-1927, 2016.

[41] S. Pashapour, A. Bozorgi-Amiri, A. Azadeh, S. F. Ghaderi, and A. Keramati, "Performance optimization of organizations considering economic resilience factors under uncertainty: A case study of a petrochemical plant," *Journal of cleaner production,* vol. 231, pp. 1526-1541, 2019.

[42] C. W. Zobel and M. Baghersad, "Analytically comparing disaster resilience across multiple dimensions," *Socio-Economic Planning Sciences,* vol. 69, p. 100678, 2020.

[43] A. W. Righi, T. A. Saurin, and P. Wachs, "A systematic literature review of resilience engineering: Research areas and a research agenda proposal," *Reliability Engineering & System Safety,* vol. 141, pp. 142-152, 2015.

[44] N. Sahebjamnia, S. A. Torabi, and S. A. Mansouri, "Building organizational resilience in the face of multiple disruptions," *International Journal of Production Economics,* vol. 197, pp. 63-83, 2018.

[45] Z. Wang, M. S. Nistor, and S. W. Pickl, "Analysis of the definitions of resilience," *IFAC-PapersOnLine,* vol. 50, no. 1, pp. 10649-10657, 2017.

[46] T. Andersson, M. Cäker, S. Tengblad, and M. Wickelgren, "Building traits for organizational resilience through balancing organizational structures," *Scandinavian Journal of Management,* vol. 35, no. 1, pp. 36-45, 2019.

[47] A. X. Sanchez, P. Osmond, and J. van der Heijden, "Are some forms of resilience more sustainable than others," *Procedia engineering,* vol. 180, pp. 881-889, 2017.

[48] A. Mehmood, "Of resilient places: planning for urban resilience," *European Planning Studies,* vol. 24, no. 2, pp. 407-419, 2016.

[49] R. Freeman, C. McMahon, and P. Godfrey, "Design of an integrated assessment of re-distributed manufacturing for the sustainable, resilient city," 2016: Springer, pp. 601-612.

[50] A. S. Kahnamouei, T. G. Bolandi, and M. R. Haghifam, "The conceptual framework of resilience and its measurement approaches in electrical power systems," in *IET Conference Publications*, 2017, vol. 2017, CP727 ed.

[51] X. Jin and X. Gu, "Option-Based Design for Resilient Manufacturing Systems," *IFAC-PapersOnLine,* Article vol. 49, no. 12, pp. 1602-1607, 2016, doi: 10.1016/j.ifacol.2016.07.809.

[52] D. Wei and K. Ji, "Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights," in *Proceedings - ISRCS 2010 - 3rd International Symposium on Resilient Control Systems*, 2010, pp. 15-22, doi: 10.1109/ISRCS.2010.5603480.

[53] C. Nan and G. Sansavini, "A quantitative method for assessing resilience of interdependent infrastructures," *Reliability Engineering and System Safety,* Article vol. 157, pp. 35-53, 2017, doi: 10.1016/j.ress.2016.08.013.

[54] A. Luo, Y. Kou, J. Liu, and T. Chen, "The resilience measure method to information systems," in *Proceedings of 2018 the 8th International Workshop on Computer Science and Engineering, WCSE 2018*, 2018, pp. 400-405.

[55] A. Kusiak, "Fundamentals of smart manufacturing: A multi-thread perspective," *Annual Reviews in Control,* Review vol. 47, pp. 214-220, 2019, doi: 10.1016/j.arcontrol.2019.02.001.

[56] K. Govindan, S. G. Azevedo, H. Carvalho, and V. Cruz-Machado, "Lean, green and resilient practices influence on supply chain performance: interpretive structural modeling approach," *International Journal of Environmental Science and Technology,* Article vol. 12, no. 1, pp. 15-34, 2015, doi: 10.1007/s13762-013-0409-7.

[57] J. R. Macdonald, C. W. Zobel, S. A. Melnyk, and S. E. Griffis, "Supply chain risk and resilience: theory building through structured experiments and simulation," *International Journal of Production Research,* Article vol. 56, no. 12, pp. 4337-4355, 2018, doi: 10.1080/00207543.2017.1421787.

[58] T.-K. Man, "Measuring and Analysing Resilience of Enterprise Architectures," 31th Twente Student Conference on IT, July 5th, 2019, University of Twente, Enschede, Netherlands, 2019 https://essay.utwente.nl/78730/

[59] C. Tarhan, C. Aydin, and V. Tecim, "How can be disaster resilience built with using sustainable development," *Procedia-Social and Behavioral Sciences,* vol. 216, pp. 452-459, 2016.

[60] E. Grandry, C. Feltus, and E. Dubois, "Conceptual Integration of enterprise architecture management and security risk management," in *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOC*, 2013, pp. 114-123, doi: 10.1109/EDOCW.2013.19.

[61] I. Band, W. Engelsman, C. Feltus, S. G. Paredes, and D. Diligens, "Modeling enterprise risk management and security with the archimate®," in "Language, The Open Group," 2015.

[62] M.-E. Iacob and H. Jonkers, "Quantitative analysis of enterprise architectures," in *Interoperability of Enterprise Software and Applications*: Springer, 2006, pp. 239-252.

[63] R. Wieringa and M. Daneva, "Six strategies for generalizing software engineering theories," Science of computer programming, vol. 101, pp. 136-152, 2015.

[64] R. J. Wieringa, Design science methodology for information systems and software engineering. Springer, 2014.