SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Abstraction-decomposition space for critical infrastructure systems: A framework for infrastructure planning and resilience policies

Stig Rune Sellevåg

stig-rune.sellevag@ffi.no

https://orcid.org/0000-0002-2309-8464

Total Defence Division, Norwegian Defence Research Establishment (FFI), Gunnar Randers vei 42, 2007, Kjeller, Norway

Abstract

The objective of this work has been to propose a framework that will aid governments with the development of more coherent and effective infrastructure planning and resilience policies through a system-of-systems approach that is grounded in theory for complex sociotechnical systems. The framework has been developed by using a work domain analysis (WDA). The WDA consists of an abstraction hierarchy analysis and a part-whole decomposition. Together, the abstraction hierarchy and the part-whole description form the abstraction-decomposition space (ADS) for which the system constraints apply. By imposing constraints, the WDA promotes design for adaptation where actors within the system are allowed to adapt their behaviour as they find appropriate without violating the system's constraints. The proposed ADS consists of five levels of abstraction and four levels of decomposition. By applying the ADS, it will aid decision making related to the overall purposes of the critical infrastructure system, the values and priority measures that are used to assess the system's progress towards the functional purposes, as well as formulation of infrastructure needs that are necessary to achieve the functional purposes. The framework is formative in the sense that it reveals how work can be done in the critical infrastructure system. This is important because it is not feasible to prescribe, describe and risk assess all possibilities for action that are available in complex sociotechnical systems, especially when dealing with unforeseen events. Future research should focus on finding science-based yet useful in practice ways for establishing values and priority measures that encompass sustainability issues and resilience standards.

Keywords:

resilience, adaptation, critical infrastructures, national security, work domain analysis

Article info
Received: 20 September 2021
Revised: 14 February 2022
Accepted: 18 February 2022
Available online: 20 April 2022
Citation: Sellevåg, S.R. (2022) 'Abstraction-decomposition space for critical infrastructure systems: A framework for infrastructure planning and resilience policies', Security and Defence Quarterly, 39(3), pp. 6–20. doi: 10.35467/sdq/146789.

Introduction

The maintenance of vital societal functions and the supply of essential services by critical infrastructures under pressing conditions and without major failure is of utmost importance to our society. However, critical infrastructures are vulnerable to a multitude of stresses. Lessons from disasters like large-scale power outages (Anderson *et al.*, 2007; Busby *et al.*, 2021), terrorist attacks (Santos, 2006), cyber-attacks (Ghafur *et al.*, 2019) and the still ongoing covid-19 pandemic (Goel, Saunoris, and Goel, 2021) have shown that disruption of infrastructure-based services can directly or indirectly affect other critical infrastructures through a complicated web of interdependencies; not only affecting the national and global economy, but also our national security (Lewis *et al.*, 2013). The situation is exacerbated not only by mitigating the impacts of climate change, but also by the proliferation of digital technologies that continue to add complexity to our critical infrastructures as well as novel hybrid threats (Cullen and Reichborn-Kjennerud, 2017; Giannopoulos, Smith, and Theocharidou, 2021). Understanding the fragility induced by multiple interdependencies and improving the resilience of critical infrastructures therefore becomes a matter of urgency and a priority for national security (Chang, 2009; Helbing, 2013; Oughton *et al.*, 2018; Rinaldi, *et al.*, 2001; Vespignani, 2010). At the 2021 Brussels Summit, NATO Member States therefore agreed to enhance their resilience and to "develop a proposal to establish, assess, review and monitor resilience objectives to guide nationally-developed resilience goals and implementation plans" (NATO, 2021a). However, NATO Allies do not provide any guidance on how to do so in the Summit Communiqué, which merely states that it "will be up to each individual ally to determine how to establish and meet national resilience goals and implementation plans" (NATO, 2021a).

Critical infrastructures undergo constant interaction and exchange with their economic, social and natural environments. In addition, in free market economies, there is no single entity in control of the system. Critical infrastructures are therefore often characterised as complex sociotechnical systems (Oughton *et al.*, 2018). Despite this insight since the seminal work by Rinaldi *et al.* (2001), conventional critical infrastructure protection strategies where risks are analysed, evaluated and treated individually as *e.g.* implied by the ISO 31000 standard, are still used. With increasing interconnectedness between critical infrastructure sectors following digital transformation and electrification, such strategies may lead to siloed risk management and are at the risk of becoming insufficient (Helbing, 2013). The situation is exacerbated by the historically fragmented governance of critical infrastructures spanning several government departments (Oughton *et al.*, 2018). Future strategies to strengthen the capability of critical infrastructures to cope with disruptions should therefore build on the principles of resilience and adaptation (Hollnagel, Woods, and Leveson, 2006; Schulman, 2022; Woods, 2020).

Following Oughton *et al.* (2018), we argue that the implementation of resilience and adaptation strategies for critical infrastructures at the national level is hampered by the low availability of easy-to-use frameworks building upon complexity theory-based system-of-systems approaches. Furthermore, as argued by Dolan (2018), with the absence of a shared strategic vision of the desired outcomes that infrastructure is expected to enable (purpose), it is not possible to fully evaluate system performance gaps or assess infrastructure needs. There is therefore a need for long-term, system-scale and cross-sector approaches to critical infrastructures resilience and planning efforts (Otto *et al.*, 2016).

Cognitive work analysis (CWA) is a well-suited framework for the analysis, design and evaluation of complex sociotechnical systems (Naikar, 2013; Vicente, 1999). In particular, CWA defines the work demands for such systems in terms of constraints on actors,

thus placing limits on behaviour (Naikar, 2013). Despite such limits, there are still many degrees of freedom for action in complex sociotechnical systems; in fact more than can be prescribed *a priori*. CWA therefore promotes designing for adaptation where actors within the system are allowed to adapt their behaviour as they find appropriate without violating the system's constraints (Naikar, 2013). CWA is thus formative in the sense that it reveals how work can be done in a system. This is important because it is not feasible to prescribe, describe and risk assess all possibilities for action that are available in complex sociotechnical systems, especially when dealing with unforeseen events.

In this study, we propose CWA, in particular the work domain analysis (WDA) phase of CWA, as an approach to support critical infrastructure public policy decision-making at the national level. The novelty of this approach is that it will aid decision-makers with the development of more coherent and effective infrastructure planning and resilience policies through a system-of-systems approach that is grounded in theory for complex sociotechnical systems. In particular, the proposed approach will aid decision-making related to the overall purposes of the critical infrastructure system, the values and priority measures that are used to assess the system's progress towards the functional purposes, as well as formulation of infrastructure needs that are necessary to achieve the functional purposes. The proposed approach complements and can be used in conjunction with other proposed approaches for infrastructure public policy decision-making (Dolan, 2018; Oughton *et al.*, 2018). To demonstrate the broad applicability of the framework, both civilian and defence-related critical infrastructure use cases will be exemplified.

Methods

Work Domain Analysis

The CWA framework consists of five phases: work domain analysis (WDA), control task analysis, strategies analysis, social organisation and cooperation analysis and worker competencies analysis (Naikar, 2013; Vicente, 1999). Only the WDA phase has been applied in this work. In the WDA phase, the functional structure of the system is described by identifying the purposes, values and priorities, functions, processes and object-related constraints of the work domain. As such, the WDA describe the fundamental reasons and resources for the different actors' behaviour within the work domain (Naikar, 2013).

The WDA consists of an abstraction hierarchy analysis and a part-whole decomposition. Together, the abstraction hierarchy and the part-whole description form the abstraction-decomposition space (ADS) for which the system constraints apply. Since WDA is event-independent, the identified system constraints, *e.g.* the identified values and priorities, are applicable to many different situations, including unanticipated events.

The abstraction dimension of the WDA spans the set of concepts for describing the functional structure of the system (Naikar, 2013; Vicente, 1999). This is done by employing the abstraction hierarchy method which uses means-ends links to show relationships between nodes across different levels of abstraction. Linked nodes above a node under consideration (the 'what') describe 'why' that node is required, while linked nodes below the node describe 'how' the node is achieved. In the context of this study, a node can *e.g.* be a critical infrastructure system or an infrastructure asset. By applying the how-what-why triad four times, an abstraction hierarchy for identification of critical entities providing essential services for maintaining vital societal functions can be developed as illustrated in Figure 1.

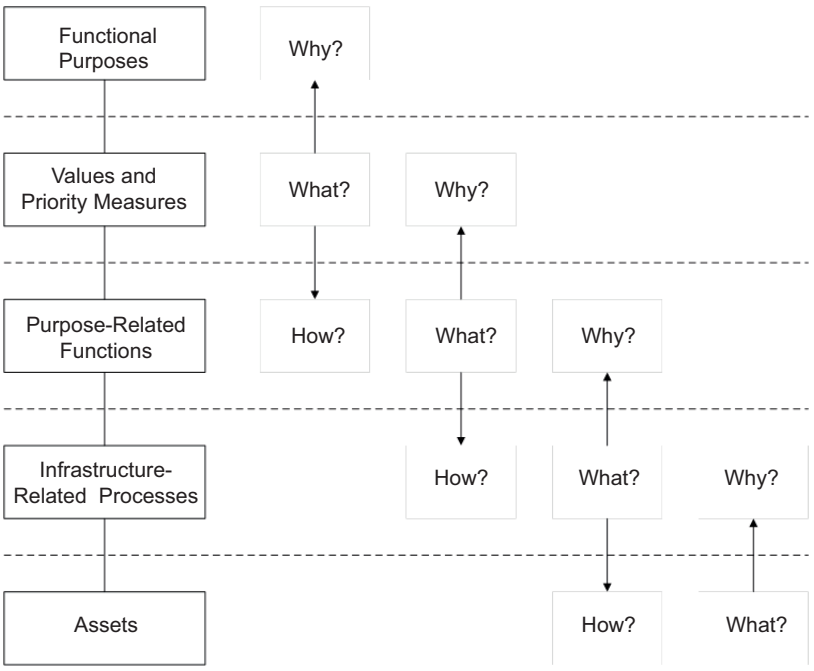

Figure 1. Five-level abstraction hierarchy with the how-what-why triad illustrated.

The abstraction hierarchy proposed in this work is a modification of the usual five-level abstraction hierarchy (Vicente, 1999), and consists of the following conceptual levels:

1. *Functional purposes* – The overall purposes of the system;
2. *Values and priority measures* – The values that are assessed and used to measure the system's progress towards the functional purposes;
3. *Purpose-related functions* – The generalised functions of the system that are necessary to achieve the functional purposes;
4. *Infrastructure-related processes* – The functional capabilities of the system's assets that enable the purpose-related functions;
5. *Assets* – The system's assets that undertake the infrastructure-related processes;

Here, the original term 'physical objects' has been replaced by 'assets,' which is considered to be more appropriate for describing infrastructures. This abstraction hierarchy is therefore consistent with the definition of infrastructure suggested by Oughton *et al.* (2018), *i.e.* "the coordinated operation and management of a group of physical assets to perform a range of processes, thereby providing infrastructure services to users".

It is important to note that the representations at the different levels of abstraction should be categories and not specific instances of a category. Furthermore, the means-ends relationships should be structural and not action means-ends relations (Naikar, 2013; Vicente, 1999). Consequently, nouns rather than verbs should be used to describe the different functions and objects in the work domain.

The decomposition dimension of the WDA provides levels of granularity for describing the functional purpose of the system (Naikar, 2013; Vicente, 1999). The levels of decomposition are connected by so-called part-whole relations; *i.e.*, nodes at lower levels are functional parts of those at higher levels. For the purpose of this work and given the

objectives of the proposed European Union (EU) COM(2020) 829 directive (European Commission, 2020), the following levels of decomposition are found expedient for describing vital societal functions:

1. Whole system;
2. Sectors;
3. Sub-sectors;
4. Types of entities.

The fourth level, *types of entities*, describes the types of public or private entities that provide the assets, and will aid the identification of critical entities in accordance with Article 5 of the proposed EU COM(2020) 829 directive (European Commission, 2020).

Selection of Use Cases

To illustrate the usability and the different aspects of the proposed framework, several critical infrastructure use cases were selected. EU critical infrastructures, as described in the proposed EU COM(2020) 829 directive (European Commission, 2020), were selected as the main use case in this study. This use case is considered relevant for many country-specific applications of the framework. In addition, Norway and the United Kingdom (UK) were included as use cases for the discussion of qualitative and quantitative values and priority measures, respectively, while NATO's seven baseline requirements (NATO, 2021b) were used to illustrate the use of the framework for defence-related use cases. UK was selected out of relevance for the discussion of quantitative values and priority measures, while Norway was selected out of convenience.

Results and Discussion

Abstraction-Decomposition Space Applied to Critical Infrastructure Systems

The ADS for describing critical infrastructure systems is summarised in Table 1. As argued by Vicente (1999), each cell in the ADS offers a complete but different representation of the same work domain. The top left cell in Table 1 represents the functional purposes of the whole system, while the bottom right cell describes the types of entities for all of the individual assets in the system. It is often not necessary to populate the whole table since the solution is often found along the diagonal of the ADS as indicated by the shaded cells in Table 1. Still, it can be useful to define specific values and priority measures, *e.g.* resilience criteria, for the identified sectors, sub-sectors and types of entities.

In the following, the use of the ADS will be exemplified and discussed with critical infrastructures in the UK and the EU as use cases. Examples from Norway and NATO will be leveraged as well. As a starting point for the discussion, the work domain (the whole system) is to be considered as an open sociotechnical system consisting of critical infrastructure systems that are to be identified. The work domain is therefore to be considered as a system of systems.

Functional Purposes

The first level of abstraction in the ADS describes the purposes that the system, *i.e.* the system of systems, serves in its environment. That is, the system exists because the

Decomposition / Abstraction	Whole system	Sectors	Sub-sectors	Types of entities
Functional purposes				
Values and priority measures				
Purpose-related functions				
Infrastructure-related processes				
Assets				

Table 1. Abstraction-decomposition space for critical infrastructure systems with five levels of abstraction and four levels of decomposition. The shaded cells illustrate the relationship between abstraction and decomposition levels for critical infrastructure systems.

environment has certain needs and the system can fulfil these needs. As argued by Dolan (2018), such a strategic need assessment requires a clearly articulated systemic vision comprising sector-, solution- and technology-neutral desired outcomes which is understood and accepted. This is important in a defence and security context. First, it will be difficult to protect a system if the functional purposes of the system are not fully understood and accepted. Secondly, any solution- or technology-biased purpose description will shape the decisions made for the subsequent abstraction levels. Poor decision-making can result in "lock-in" effects that put the infrastructure systems on long-term path-dependent trajectories that can be hard to break away from due to, *e.g.* the financial or technological hurdles involved (Oughton *et al.*, 2018).

Depending upon how the needs are described, who is the reference object for the need and which constraints are provided, different models of a system can emerge. For example, the purpose of the system can be to *safeguard the basic needs of the population in the society*. Here, one may say it is the population in the society that frames the constraints for the work domain. A different functional purpose can be to *maintain national security, national defence and the functioning of the state*. In this case, the national security act would provide a constraint on the work domain. A third functional purpose could be to *safeguard the nation as a democracy and a state based on the rule of law and universal respect for human rights* in accordance with the nation's constitution. In this case, the constitution provides the constraint. A fourth type of need could be to *maintain vital societal functions or economic activities in the EU internal marked* in accordance with Article 1 of the proposed EU COM(2020) 829 directive (European Commission, 2020); consequently, the constraint is given by the directive. A last example of a need is the need to *resist armed attack* as described by Article 3 in The North Atlantic Treaty. Here, it is the Treaty that provides the constraints on the work domain. Understanding the functional purposes of the system is therefore essential for applying the ADS.

Values and Priority Measures

The values and priority measures level of abstraction provides two types of criteria: The first is measures for how well the system is progressing towards its functional purposes, while the second is criteria for comparing, prioritising and directing resources to the various purpose-related functions so that the functional purposes of the work system are fulfilled. Examples of the first type at the national level could be sustainability measures

or levels of services, while the second could be resilience criteria. Since the criteria at this level of abstraction are invariants or relatively stable properties of the work domain, they provide guidance for reasoning from first principles when the system is confronted with stressful, unanticipated events.

Values and priority measures at the national level (whole system) may be difficult to describe quantitatively; such criteria are therefore usually qualitative. Taking the Norwegian Act relating to national security as an example, the values and priority measures for the system as a whole could be described as *protection of national security interests*. Such interests are defined as "Norway's sovereignty, territorial integrity and democratic system of government, and general political security interests related to a) the activities, security and freedom of action of the highest state bodies; b) defence, security and contingency preparedness; c) relations with other states and international organisations; d) economic stability and freedom of action; e) fundamental national functions and the basic security of the population" (Security Act, 2019). In the Norwegian security act, fundamental national functions are defined as "services, production and other types of activity which are of such importance that a complete or partial loss of the function would have consequences for the State's ability to protect national security interests" (Security Act, 2019). For the proposed EU COM (2020) 829 directive, the values and priority measures could be described as *ensure the provision of essential services* for the maintenance of vital societal functions or economic activities in the EU internal marked (European Commission, 2020).

Quantitative performance measures for infrastructure sectors are possible and have been taken by the UK National Infrastructure Commission (NIC) (National Infrastructure Commission, 2018). These performance measures provide clear guidance for how to assess and measure each infrastructure sector's performance. For this purpose, Dolan *et al.* (2016) have proposed a conceptual approach for identifying outcome-oriented performance indicators for infrastructures, which has been applied by Carhart *et al.* (2016). However, because of infrastructure interdependencies, performance loss in one infrastructure sector may influence the performance of other infrastructure sectors. It is therefore necessary to define desired outcomes for the system as whole and not at a sector-by-sector level in order to define meaningful outcome-oriented performance indicators to evaluate cross-sectoral performance (Dolan *et al.*, 2016). Indicators at the sectoral level may still be helpful to guide the development of such whole-system performance indicators.

For example, performance measures for critical infrastructure sectors can be used to quantify resilience (Bruneau *et al.*, 2003). Although several definitions of resilience exist (Cereè, Rezgui, and Zhao, 2017; Curt and Tacnet, 2018; Haimes, 2009; Petersen *et al.*, 2020; Wied, Oehmen, and Welo, 2020), most definitions are formulated around the system's ability to reduce the chances of an undesired event and to maintain and recover its core functionality in case of disruption. By setting constraints on minimum system performance loss and recovery time before the service level is restored, risk-based resilience standards for critical infrastructure sectors can be put forward (FEMA, 2019; Poland, 2009). However, as discussed by Haimes (2009), such efforts should be contextualised to the risks to the system and their associated consequences. This calls for unified approaches to risk and resilience analysis and management (Aven, 2019). In addition, critical infrastructure sectors should undergo stress testing to evaluate whether they meet the resilience standards (Esposito *et al.*, 2020).

Resilience standards as part of the values and priority measures for critical infrastructure systems at the national level should therefore be established on the basis of the national

risk assessment. Here, it is important to take the scale of possible undesired disruptive events into consideration. Lessons from the Covid-19 pandemic have shown that the pace, duration and the geographic scale of a crisis, the interconnectedness of critical infrastructures and the associated cascading risks, and nation states' capacity to prepare and respond are all important drivers for a crisis (Collins, Florin, and Renn, 2020). Thus, these are all important factors to take into consideration when establishing resilience standards. Furthermore, it is also important to take the vulnerabilities of critical infrastructure systems into consideration in the national risk assessment, since such vulnerabilities may translate into threat scenarios if they are exploited.

As argued by both the UK NIC (National Infrastructure Commission, 2020) and the proposed EU COM(2020) 829 directive (European Commission, 2020), resilience standards for critical infrastructure systems should be government's responsibility and not the (usually) private entities providing the services. This is in agreement with the ADS proposed in this work since values and priority measures apply to the system as a whole. The UK NIC provides several reasons for this (National Infrastructure Commission, 2020): Firstly, the government will be involved when there are serious failures or risks are too high for private entities. Secondly, resilience is not properly valued on the market. Thirdly, because of interdependencies, failure to provide a service does not just affect the consumers of that particular service. Lastly, markets focus on those who can pay, while in a crisis the focus should be on those who are in need.

Purpose-Related Functions

As mentioned, purpose-related functions are functions that are necessary for fulfilling the functional purposes of the whole system. This requires coordination of the purpose-related functions in accordance with the values and priority measures. Furthermore, the functions are generalised functions to accommodate a wide variety of activities by the underlying levels of abstraction.

Purpose-related functions are typically decomposed into sectors where each sector would constitute a system. In the proposed EU COM(2020) 829 directive, the following ten sectors are identified (European Commission, 2020): (1) Energy; (2) Transport; (3) Banking; (4) Financial market infrastructures; (5) Health; (6) Drinking water; (7) Waste water; (8) Digital infrastructure; (9) Public administration; and (10) Space. These sectors can be translated into purpose-related functions by using nouns for describing the different objects of action, *e.g. provision of energy*, *provision of transportation*, *provision of banking services*, *provision of financial market infrastructure services*, *provision of health services*, *provision of drinking water*, *provision of waste water services*, *provision of digital infrastructure services*, *provision of public administration services* and *provision of space-based services*. In the context of this study, these purpose-related functions can be considered as vital societal functions because they provide essential services for the functional purposes of the EU internal market.

If we look at the functional purpose of maintaining civil preparedness in accordance with NATO's seven baseline requirements, the following purpose-related functions can be described (NATO, 2021b): (1) Provision of critical government services; (2) Provision of energy supplies; (3) Management of uncontrolled movement of people; (4) Provision of food and water resources; (5) Management of mass casualties; (6) Provision of telecommunications; and (7) Provision of transportation. Several sectors can be involved in providing the purpose-related function. In order to deal with mass casualties for example, both rescue services and the health sector are required.

Infrastructure-Related Processes

The infrastructure-related processes level of abstraction describes the functional capabilities that enable the purpose-related functions in the work domain. Taking EU critical infrastructures (European Commission, 2020) as an example, the provision of electricity, district heating and cooling, oil, gas or hydrogen all contribute to the purpose-related function *provision of energy*. Likewise, air, rail, water and road transport services enable the function *provision of transportation*.

Assets

The last level of abstraction in the proposed ADS represents the assets that enable the higher-level processes and functions. Such assets can be both physical and non-physical assets. Taking the electricity sector as an example, assets for generation, transmission, distribution, storage and supply are needed in order to provide electricity. Infrastructures can therefore be represented as networks that are interconnected with the physical and non-physical assets, where the network representation models the infrastructure-related processes and the asset representation models the components that are required for providing the processes (Goldbeck, Angeloudis, and Ochieng, 2019; Oughton *et al.*, 2018; Ouyang, 2014).

Interdependencies, object worlds and identification of critical entities

An infrastructure interdependency can be defined as a "bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other" (Rinaldi *et al.*, 2001). Such interdependencies can be of many different types, see *e.g.* Ouyang (2014) for a review. Understanding the vulnerabilities induced by multiple interdependencies is generally considered one of the major challenges when it comes to improving infrastructure resilience (Chang, 2009). If the vulnerabilities can be exploited by an adversary, the vulnerabilities will translate into threat scenarios. Mapping of assets and their interdependency relations is therefore needed for risk management and improving infrastructure resilience.

The types of interdependencies proposed by *e.g.* Rinaldi *et al.* (2001), Zimmerman (2001) and Dudenhoeffer, Permann, and Manic (2006), see also Ouyang (2014) for a review, can be considered as caused-based interdependencies. Such dependencies could be of physical, informational, geospatial, procedural or societal types. In a recent study, Goldbeck *et al.* (2019) argued that effect-based classification of interdependencies is more important for modelling purposes, since interdependencies can yield similar effects despite having different causes. For this purpose, Goldbeck *et al.* (2019) proposed four types of effect-based dependency relations: (i) stochastic failure propagation, (ii) logic, (iii) asset utilisation and (iv) resource input dependencies. A framework for characterising infrastructure dependencies has also been proposed by Carhart and Rosenberg (2016).

This study proposes that ADS can be used as a tool to frame the mapping of interdependencies to different levels of abstraction and decomposition. Figure 2 shows a simple, yet illustrative example of how the ADS can be used to map interdependencies by using the dependency relations example provided by Rinaldi *et al.* (2001) for the electricity sub-sector that is a part of EU critical infrastructures (Table 2). As can be seen, the interdependencies are of both intra-sector and inter-sector types (Carhart and Rosenberg, 2016). Such

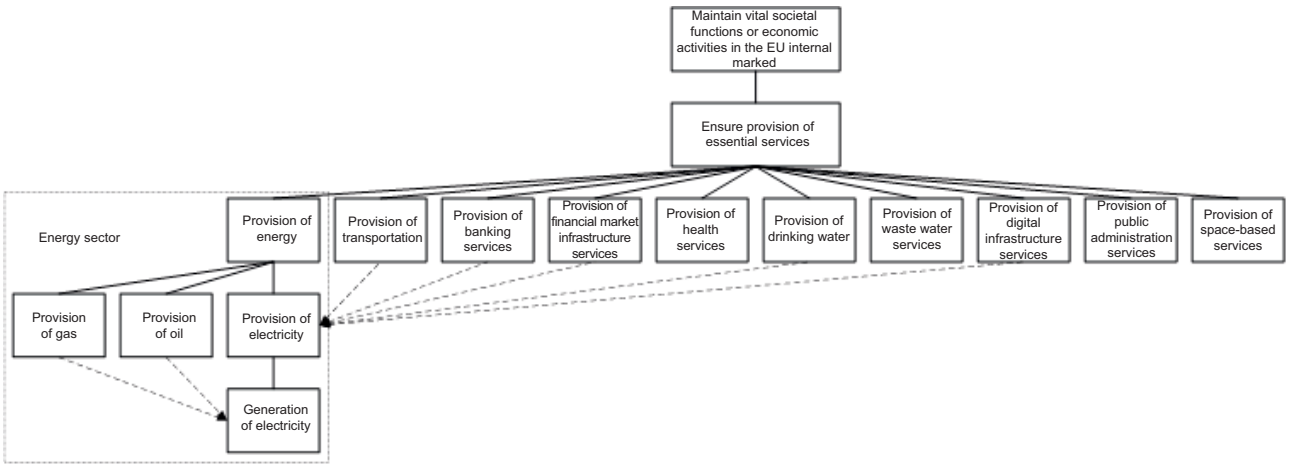

Figure 2. Simple, illustrative example of mapping of dependency relations (dashed arrows) for the electricity sub-sector using an abstraction hierarchy for EU critical infrastructures and an interdependency example provided by Rinaldi *et al.* (2001). The solid lines show the structural means-ends relationships.

interdependency mapping can inform policy and decision-making at the national level on risks across different infrastructure sectors as well as aid the identification of critical entities in accordance with the EU COM(2020) 829 directive (European Commission, 2020). It can also help inform entities to perform assessments of how their assets fit within

Table 2. Abstraction-decomposition space for EU critical infrastructures using the electricity sub-sector as an example.

Decomposition / Abstraction	Whole system	Sectors	Sub-sectors	Types of entities
Functional purposes	Maintain vital societal functions or economic activities in the EU internal marked			
Values and priority measures	Ensure provision of essential services			
Purpose-related functions		Provision of energy		
Infrastructure-related processes			Provision of electricity	
Assets				Generation; Transmission; Distribution; Storage; Supply

and are affected by a broader web of interdependencies with other entities' assets. Applying the ADS may therefore help to elucidate the structural complexity (Zio, 2016) of critical infrastructures at the national level.

Furthermore, as mentioned in the introduction, critical infrastructure systems in free market economies do not, in general, have a single entity in control of the system (Oughton *et al.*, 2018). On the contrary, the control is often distributed amongst several stakeholders and where governmental authorities have limited regulatory control. In addition, governance at the national level is often fragmented across several government departments. The UK and other countries such as Australia and New Zealand have therefore taken steps to coordinate infrastructure policy across government (Oughton *et al.*, 2018).

In the context of the ADS proposed in this work, stakeholders' interests and decision-making will occur at different levels of abstraction and decomposition. Consequently, different stakeholders will have different but overlapping views of the same system (work domain). Such views can be considered as different object worlds (Naikar, Hopcroft, and Moylan, 2005). Because of the overlap and interdependencies between different stakeholders' object worlds, changes or effects in one stakeholder's object world can propagate to other object worlds (Naikar *et al.*, 2005). Finding ways for the different stakeholders to collaborate effectively is therefore necessary for improving risk management. The ADS proposed in this work will help to elucidate and frame the object worlds of different stakeholders and decision-makers thus aiding the mapping of interdependencies and the coordination of policies across different infrastructure sectors.

Limitations

The limitations of this study pertain to the applicability of WDA in general and to critical infrastructure systems in particular. Although the usefulness of WDA has been demonstrated by many studies (Naikar, 2017), there is generally a lack of validation of such models (Rechard *et al.*, 2015). Put simply, validation deals with building the right model (Rykiel, 1996). The lack of validation also applies to this work. We therefore do not have empirical evidence for whether the methodology for WDA will result in valid and reliable ADS models of critical infrastructure systems. This needs to be investigated further. Expert opinions (Naikar *et al.*, 2005) and scenario mapping (Burns, Bryant, and Chalmers, 2001) could serve as useful methods for validating that a proposed ADS model captures all relevant domain constraints for the critical infrastructure system under study.

Conclusions

The objective of this work has been to propose a framework that will aid governments with the development of more coherent and effective infrastructure planning and resilience policies through a system-of-systems approach that is grounded in theory for complex sociotechnical systems. To this end, a novel abstraction-decomposition space (ADS) for critical infrastructure systems has been proposed on the basis of work domain analysis (WDA) (Naikar, 2013; Vicente, 1999).

The ADS consists of five levels of abstraction and four levels of decomposition. The framework is formative in the sense that it reveals how work can be done in the critical infrastructure system without violating the system's constraints established through the WDA. By imposing constraints, the ADS promotes design for adaptation where actors within the

system are allowed to adapt their behaviour as they find appropriate within the system's constraints. This is important because it is not feasible to prescribe, describe and risk assess all possibilities for action that are available in complex sociotechnical systems such as critical infrastructures, especially when dealing with unforeseen events. Efforts to strengthen the capability of critical infrastructures to cope with disruptions should therefore build on the principles of resilience and adaptation (Hollnagel *et al.*, 2006; Schulman, 2022; Woods, 2020).

In this work, we have argued that the implementation of resilience and adaptation strategies for critical infrastructures at the national level is hampered by the low availability of easy-to-use frameworks that build upon complexity theory-based system-of-systems approaches. Adding to this, the absence of a shared strategic vision of the desired outcomes that infrastructure is expected to enable will make it difficult to fully evaluate system performance gaps or assess future infrastructure needs (Dolan, 2018; Dolan *et al.*, 2016).

By applying the ADS, it will aid decision-making related to the overall purposes of the critical infrastructure system, the values and priority measures that are used to assess the system's progress towards the functional purposes, as well as formulation of infrastructure needs that are necessary to achieve the functional purposes. In addition, it will help to elucidate infrastructure interdependencies and aid the coordination of policies across different infrastructure sectors by framing the views (object worlds) of different stakeholders. This may help EU Member States and others to formulate better strategic objectives and priorities for enhancing the overall resilience of critical infrastructure systems. It may also assist governments with identification of essential services and the critical entities that deliver such services in accordance with the proposed EU COM(2020) 829 directive (European Commission, 2020).

Future research should focus on finding science-based, yet pragmatic and useful in practice, ways for establishing values and priority measures that encompass sustainability issues and resilience standards at the national level. Such criteria should be relatively stable properties of the critical infrastructure system to allow reasoning from first principles when the system is under stress due to unanticipated events, in particular black swan events.

Funding

This work was funded by the Norwegian Ministry of Defence through project grant 1619.

Data Availability Statement

Not applicable.

The author read and agreed to the published version of the manuscript.

Disclosure statement

No potential conflict of interest was reported by the author.

References

Anderson, C.W., Santos, J.R. and Haimes, Y.Y. (2007) 'A risk-based input–output methodology for measuring the effects of the August 2003 Northeast blackout', *Economic Systems Research*, 19(2), pp. 183–204. doi: 10.1080/09535310701330233.

Aven, T. (2019) 'The call for a shift from risk to resilience: What does it mean?', *Risk Analysis*, 39(6), pp. 1196–1203. doi: 10.1111/risa.13247.

Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O'Rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A. and von Winterfeldt, D. (2003) 'A framework to quantitatively assess and enhance the seismic resilience of communities', *Earthquake Spectra*, 19(4), pp. 733–752. doi: 10.1193/1.1623497.

Burns, C.M., Bryant, D.J. and Chalmers, B.A. (2001) 'Scenario mapping with work domain analysis', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 45(4), pp. 424–428. doi: 10.1177/154193120104500434.

Busby, J.W., Baker, K., Bazilian, M.D., Gilbert, A.Q., Grubert, E., Rai, V., Rhodes, J.D., Shidore, S., Smith, C.A. and Webber, M.E. (2021) 'Cascading risks: Understanding the 2021 winter blackout in Texas', *Energy Research & Social Science*, 77, 102106. doi: 10.1016/j.erss.2021.102106.

Carhart, N. and Rosenberg, G. (2016) 'A framework for characterising infrastructure interdependencies', *International Journal of Complexity in Applied Science and Technology*, 1, pp. 35–60. doi: 10.1504/IJCAST.2016.10002359.

Carhart, N.J., Bouch, C., Walsh, C.L. and Dolan, T. (2016) 'Applying a new concept for strategic performance indicators', *Infrastructure Asset Management*, 3(4), pp. 143–153. doi: 10.1680/jinam.16.00016.

Cerè, G., Rezgui, Y. and Zhao, W. (2017) 'Critical review of existing built environment resilience frameworks: Directions for future research', *International Journal of Disaster Risk Reduction*, 25, pp. 173–189. doi: 10.1016/j.ijdrr.2017.09.018.

Chang, S.E. (2009) 'Infrastructure resilience to disasters', *The Bridge*, 39, pp. 36–41.

Collins, A., Florin, M.-V. and Renn, O. (2020) 'COVID-19 risk governance: Drivers, responses and lessons to be learned', *Journal of Risk Research*, 23(7–8), pp. 1073–1082. doi: 10.1080/13669877.2020.1760332.

Cullen, P.J. and Reichborn-Kjennerud, E. (2017) *MCDC countering hybrid warfare project: Understanding hybrid warfare. A multinational capability development campaign project*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf (Accessed: 15 March 2022).

Curt, C. and Tacnet, J.-M. (2018) 'Resilience of critical infrastructures: Review and analysis of current approaches', *Risk Analysis*, 38(11), pp. 2441–2458. doi: 10.1111/risa.13166.

Dolan, T. (2018) 'Briefing: A systemic framework for infrastructure need assessment', *Proceedings of the Institution of Civil Engineers – Smart Infrastructure and Construction*, 171(2), pp. 45–53. doi: 10.1680/jsmic.18.00006.

Dolan, T., Walsh, C.L., Bouch, C. and Carhart, N.J. (2016) 'A conceptual approach to strategic performance indicators', *Infrastructure Asset Management*, 3(4), pp. 132–142. doi: 10.1680/jinam.16.00015.

Dudenhoeffer, D.D., Permann, M.R. and Manic, M. (2006) 'CIMS: A framework for infrastructure interdependency modeling and analysis', *Proceedings of the 2006 Winter Simulation Conference*, 3–6 December 2006, pp. 478–485.

Esposito, S., Stojadinović, B., Babič, A., Dolšek, M., Iqbal, S., Selva, J., Broccardo, M., Mignan, A. and Giardini, D. (2020) 'Risk-based multilevel methodology to stress test critical infrastructure systems', *Journal of Infrastructure Systems*, 26(1), 04019035. doi: 10.1061/(ASCE)IS.1943-555X.0000520.

European Commission (2020) *Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities*. (COM(2020) 829 final). Brussels: European Commission.

FEMA (2019) *2019 National Threat and Hazard Identifiaction and Risk Assessment (THIRA). Overview and methodology*. U.S. Department of Homeland Security. Available at: https://www.fema.gov/sites/default/files/2020-06/fema_national-thira-overview-methodology_2019_0.pdf (Accessed: 15 March 2022).

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. and Aylin, P. (2019) 'A retrospective impact analysis of the WannaCry cyberattack on the NHS', *NPJ Digital Medicine*, 2(98). doi: 10.1038/s41746-019-0161-6.

Giannopoulos, G., Smith, H. and Theocharidou, M. (2021) *The landscape of hybrid threats: A conceptual model*. (EUR 30585 EN). Luxembourg: Publications Office of the European Union.

Goel, R.K., Saunoris, J.W. and Goel, S.S. (2021) 'Supply chain performance and economic growth: The impact of COVID-19 disruptions', *Journal of Policy Modeling*, 43(2), pp. 298–316. doi: 10.1016/j.jpolmod.2021.01.003.

Goldbeck, N., Angeloudis, P. and Ochieng, W.Y. (2019) 'Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models', *Reliability Engineering and System Safety*, 188, pp. 62–79. doi: 10.1016/j.ress.2019.03.007.

Haimes, Y.Y. (2009) 'On the definition of resilience in systems', *Risk Analysis*, 29(4), pp. 498–501. doi: 10.1111/j.1539-6924.2009.01216.x.

Helbing, D. (2013) 'Globally networked risks and how to respond', *Nature*, 497(7447), pp. 51–59. doi: 10.1038/nature12047.

Hollnagel, E., Woods, D. and Leveson, N. (ed.). (2006) *Resilience engineering: Concepts and precepts*. Boca Raton: CRC Press.

Lewis, A.M., Ward, D., Cyra, L. and Kourti, N. (2013) 'European reference network for critical infrastructure protection', *International Journal of Critical Infrastructure Protection*, 6(1), pp. 51–60. doi: 10.1016/j.ijcip.2013.02.004.

Naikar, N. (2013) *Work domain analysis: Concepts, guidelines, and cases*. Boca Raton: CRC Press.

Naikar, N. (2017) 'Cognitive work analysis: An influential legacy extending beyond human factors and engineering', *Applied Ergonomics*, 59, pp. 528–540. doi: 10.1016/j.apergo.2016.06.001.

Naikar, N., Hopcroft, R. and Moylan, A. (2005) *Work domain analysis: Theoretical concepts and methodology*. (DSTO-TR-1665). Australia: Air Operations Division, Defence Science and Technology Organisation.

National Infrastructure Commission (2018) *National infrastructure assessment*. Available at: https://nic.org.uk/app/uploads/CCS001_CCS0618917350-001_NIC-NIA_Accessible-1.pdf (Accessed: 15 March 2022).

National Infrastructure Commission (2020) *Anticipate, react, recover. Resilient infrastructure systems*. Available at: https://nic.org.uk/app/uploads/Anticipate-React-Recover-28-May-2020.pdf (Accessed: 15 March 2022).

NATO (2021a) *Brussels Summit Communiqué*. Available at: https://www.nato.int/cps/en/natohq/news_185000.htm (Accessed: 5 February 2022).

NATO (2021b) *Civil preparedness*. Available at: https://www.nato.int/cps/en/natohq/topics_49158.htm (Accessed: 14 May 2021).

Otto, A., Hall, J.W., Hickford, A.J., Nicholls, R.J., Alderson, D., Barr, S. and Tran, M. (2016) 'A quantified system-of-systems modeling framework for robust national infrastructure planning', *IEEE Systems Journal*, 10(2), pp. 385–396. doi: 10.1109/JSYST.2014.2361157.

Oughton, E.J., Usher, W., Tyler, P. and Hall, J.W. (2018) 'Infrastructure as a complex adaptive system', *Complexity*, 2018. doi: 10.1155/2018/3427826.

Ouyang, M. (2014) 'Review on modeling and simulation of interdependent critical infrastructure systems', *Reliability Engineering and System Safety*, 121, pp. 43–60. doi: 10.1016/j.ress.2013.06.040.

Petersen, L., Lange, D. and Theocharidou, M. (2020) 'Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators', *Reliability Engineering & System Safety*, 199. doi: 10.1016/j.ress.2020.106872.

Poland, C. (2009) *The resilient city: Defining what San Francisco needs from its seismic mitigation policies*. San Francisco Planning + Urban Research Association (SPUR). Available at: https://www.spur.org/publications/spur-report/2009-02-01/defining-resilience (Accessed: 15 March 2022).

Rechard, J., Bignon, A., Berruet, P. and Morineau, T. (2015) 'Verification and validation of a work domain analysis with turing machine task analysis', *Applied Ergonomics*, 47, pp. 265–273. doi: 10.1016/j.apergo.2014.10.012.

Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001) 'Identifying, understanding, and analyzing critical infrastructure interdependencies', *IEEE Control Systems Magazine*, 21, pp. 11–25. doi: 10.1109/37.969131.

Rykiel, E.J. (1996) 'Testing ecological models: The meaning of validation', *Ecological Modelling*, 90(3), pp. 229–244. doi: 10.1016/0304-3800(95)00152-2.

Santos, J.R. (2006) 'Inoperability input-output modeling of disruptions to interdependent economic systems', *Systems Engineering*, 9(1), pp. 20–34. doi: 10.1002/sys.20040.

Schulman, P.R. (2022) 'Reliability, uncertainty and the management of error: New perspectives in the COVID-19 era', *Journal of Contingencies and Crisis Management*, 30, pp. 92–101. doi: 10.1111/1468-5973.12356.

Security Act (2019) *Act relating to national security*. Available at: https://lovdata.no/dokument/NLE/lov/2018-06-01-24 (Accessed: 15 March 2022).

Vespignani, A. (2010) 'The fragility of interdependency', *Nature*, 464, pp. 984–985. doi: 10.1038/464984a.

Vicente, K.J. (1999) *Cognitive work analysis. Toward safe, productive, and healthy computer-based work*. Boca Raton: CRC Press.

Wied, M., Oehmen, J. and Welo, T. (2020) 'Conceptualizing resilience in engineering systems: An analysis of the literature', *Systems Engineering*, 23(1), pp. 3–13. doi: 10.1002/sys.21491.

Woods, D.D. (2020) 'The strategic agility gap: How organizations are slow and stale to adapt in turbulent worlds', in B. Journé, H. Laroche, C. Bieder, and C. Gilbert (eds.), *Human and organisational factors: Practices and strategies for a changing world.* Cham: Springer International Publishing, pp. 95–104.

Zimmerman, R. (2001) 'Social implications of infrastructure network interactions', *Journal of Urban Technology*, 8(3), pp. 97–119. doi: 10.1080/106307301753430764.

Zio, E. (2016) 'Challenges in the vulnerability and risk analysis of critical infrastructures', *Reliability Engineering and System Safety*, 152, pp. 137–150. doi: 10.1016/j.ress.2016.02.009.