Resilient Cities and Structures 4 (2025) 71–82

Contents lists available at ScienceDirect

Resilient Cities and Structures

journal homepage: www.elsevier.com/locate/rcns

Full Length Article

# A robustness assessment approach for transportation networks with cyber-physical interdependencies

Konstantinos Ntafloukas[a,*], Liliana Pasquale[b], Beatriz Martinez-Pastor[a], Daniel P. McCrum[a]

[a] *School of Civil Engineering, University College Dublin, D07 R2WY, Dublin, Ireland*
[b] *School of Computer Science, University College Dublin, D07 R2WY, Dublin, Ireland*

## ARTICLE INFO

*Keywords:*
Transportation network
Cyber-physical
Robustness
Interdependencies
Natural hazards
Robustness improvement indicator

## ABSTRACT

While in the past the robustness of transportation networks was studied considering the cyber and physical space as isolated environments this is no longer the case. Integrating the Internet of Things devices in the sensing area of transportation infrastructure has resulted in ubiquitous cyber-physical systems and increasing interdependencies between the physical and cyber networks. As a result, the robustness of transportation networks relies on the uninterrupted serviceability of physical and cyber networks. Current studies on interdependent networks overlook the civil engineering aspect of cyber-physical systems. Firstly, they rely on the assumption of a uniform and strong level of interdependency. That is, once a node within a network fails its counterpart fails immediately. Current studies overlook the impact of earthquake and other natural hazards on the operation of modern transportation infrastructure, that now serve as a cyber-physical system. The last is responsible not only for the physical operation (e.g., flow of vehicles) but also for the continuous data transmission and subsequently the cyber operation of the entire transportation network. Therefore, the robustness of modern transportation networks should be modelled from a new cyber-physical perspective that includes civil engineering aspects. In this paper, we propose a new robustness assessment approach for modern transportation networks and their underlying interdependent physical and cyber network, subjected to earthquake events. The novelty relies on the modelling of interdependent networks, in the form of a graph, based on their interdependency levels. We associate the serviceability level of the coupled physical and cyber network with the damage states induced by earthquake events. Robustness is then measured as a degradation of the cyber-physical serviceability level. The application of the approach is demonstrated by studying an illustrative transportation network using seismic data from real-world transportation infrastructure. Furthermore, we propose the integration of a robustness improvement indicator based on physical and cyber attributes to enhance the cyber-physical serviceability level. Results indicate an improvement in robustness level (i.e., 41 %) by adopting the proposed robustness improvement indicator. The usefulness of our approach is highlighted by comparing it with other methods that consider strong interdependencies and key node protection strategies. The approach is of interest to stakeholders who are attempting to incorporate cyber-physical systems into civil engineering systems.

## 1. Introduction

Transportation networks serve as fundamental backbones of society. Day-to-day activities rely on the undisrupted operation of urban transportation infrastructure (e.g., bridges) as integral parts of a transportation network [1]. Therefore, research has focused on the robustness assessment of public transportation networks as their ability to resist disruptions (e.g., traffic accidents) and maintain the predesigned serviceability level without significant reduction [2]. Especially in today's complex systems such as infrastructure networks that are vulnerable to a variety of threats, the study of robustness, resilience and other key concepts (e.g. recoverability) is of paramount importance [3]. Until recently, the cyber (e.g., monitoring and sensing devices) and physical (e.g., bridge structure) space were treated as isolated environments, considering that any disruption in one space will not impact the other [4]. Transportation networks are mainly constituted of civil engineering systems (e.g., bridges, roads, etc.) and, thus, the physical space was considered the primary source of threat (e.g., terrorism bombing, natural hazards, etc.) against robustness [5,6] or any other engineering concept (e.g., resilience) [7]. For example, bridges as a core engineering system of a transportation network are highly susceptible to a variety of natural hazards (e.g., floods, earthquake) [8] .However, new studies highlight that cyber-physical attacks can impact the physical space (e.g., shut down of infrastructure) and degrade its serviceability level

---

[*] Corresponding author.
*E-mail address:* konstantinos.ntafloukas@ucdconnect.ie (K. Ntafloukas).

https://doi.org/10.1016/j.rcns.2025.02.005
Received 20 December 2024; Received in revised form 25 February 2025; Accepted 25 February 2025

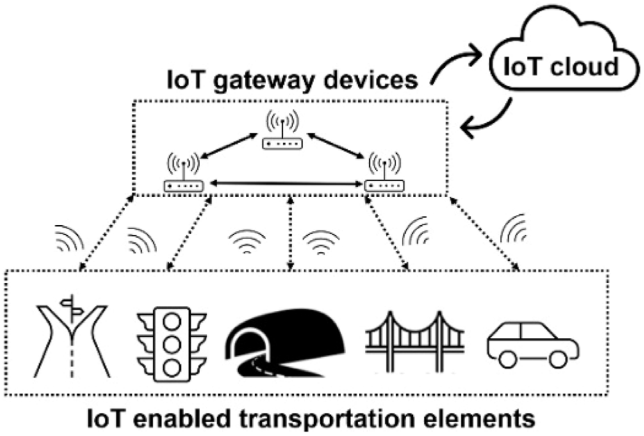

**Fig. 1.** IoT architecture based on IoT transportation elements, gateways and cloud.

after successfully exploiting cyber vulnerabilities [9]. For example, the European Union Agency for Cybersecurity reported a two-days Denial of Services attack (DoS) against the Swedish Transport Administration [10]. The cyber-physical attack resulted in major delays and degraded services to customers. Other cyber-physical attacks (e.g., Denial of Services attack) against the Internet of Things-based wireless sensor network (i.e., IoT-based WSN) of critical transportation infrastructure (i.e., IoT-enabled transportation infrastructure) have been described in previous research studies [11,12]. IoT-based WSN has been used to upgrade traditional civil engineering services (e.g., wireless structural monitoring [13], traffic monitoring [14]). Furthermore, the deployment of IoT devices (e.g., sensors) in sensing areas of critical transportation infrastructure (e.g., the deck of a bridge) enables the collection and transmission of data and the continual communication of interacting transportation elements (vehicle-to-vehicle or vehicle-to-infrastructure communication) [15,16]. Integrating the physical world with computational facilities enables critical transportation infrastructure and networks to serve as cyber-physical systems and networks with complex interdependencies.

Indeed, significant focus has been given on studying these complex interdependencies of cyber-physical systems as the operational state of each space affects or is correlated with the other [17,18]. The existence of interdependencies is due to the integration of sensing, network and application layer as the fundamental three IoT layer architecture [19]. IoT architecture relies on the data processing and collection from IoT devices, such as sensors and actuators embedded in transportation infrastructure, and data routing to the cloud through gateway devices, as shown in Fig. 1. Specifically, IoT gateway devices play a crucial role in these cyber networks, as they mediate between sensors and cloud data centres and facilitate the data flow through them [20]. Due to the significant amount of data, the gateway performs significant tasks, such as collecting and filtering unnecessary data by uploading only the necessary ones to the cloud or data centres [21,22] as well as individually managing the sensing network based on processed data of sensing networks [23–25].

Therefore, in the transportation domain, the serviceability level of an entire transportation network relies on the uninterrupted operation of IoT-enabled transportation infrastructure in both physical and cyber space, as its integral parts. Specifically, the operation of a physical network relies on uninterrupted traffic flow. Similarly, the operation of a cyber network relies on the uninterrupted process of traffic flow data through gateway devices that can intelligently communicate between them and manage sensing networks [26,27]. However, the vulnerability of IoT-enabled transportation infrastructure, such as civil engineering systems, to natural hazards jeopardizes their operation in physical space [28]. For example, the serviceability of the physical network, as a percentage of the operational level in terms of traffic flow, is highly susceptible to earthquake events [29]. Especially, transportation infrastructure, such as bridges without adequate seismic detailing (i.e., earlier design codes) in high seismic risk regions, are threatened even by collapse and loss of their physical serviceability level [30]. Therefore, understanding their performance under physical threats is of critical importance, as road infrastructure networks play a crucial role in emergency response situations [31]. Similarly, the serviceability of the cyber network, for IoT applications related to traffic flow relies on the continuous feed and processing of data to manage the sensing networks and IoT-enabled transportation infrastructure (e.g., mobile smart vehicles [32] etc.). However, data routing relies on the physical network's constant operation and the uninterrupted traffic flow of IoT-enabled transportation infrastructure. Delays in response time or missing data can result in an engineering system in a network bottleneck with negative impacts (e.g., traffic delays) [33]. The ability of IoT systems to provide reliable services depends on the quality and quantity of collected data and, therefore in the avoidance of missing data [34], the quality of sensors as well as the avoidance of hardware malfunction after the event [35,36].

Contrary to the physical serviceability level of a transportation infrastructure related to its structural condition (i.e., physical damage state), an IoT gateway may maintain its hardware condition but cannot provide the predesigned level of services. Therefore, the basic assumption of the continuous presence of vehicles and users that feed the IoT gateway with data is unrealistic, as it depends both on the unforeseen dynamic nature of the transportation network [37], and on the post-event physical serviceability level of transportation infrastructure subjected to earthquake events. Management of IoT-enabled transportation infrastructure from gateway devices and the necessity of gateway devices for continuous data feed has led to cyber-physical interdependencies. The existence of emerging cyber-physical interdependencies necessitates the study of the robustness of transportation networks from a new cyber-physical perspective.

The deep coupling of cyber-physical systems has unleashed new potential for transportation domain. The vision of a smart city governed by cyber-physical systems in several sectors related to transportation domain (e.g., automated vehicles, supply chain etc.) has been widely studied from a theoretical perspective [38]. Security issues and threats (e.g., Denial of Services attack) that threaten the operation of these systems and subsequently of an entire network (i.e., transportation network) have been detailed. Existing research and knowledge in security domain from previous standalone computing systems facilitates the transition to cyber-physical systems. However, when the coupling of cyber world with the physical world materialized, it is not only the security issues that threaten the entire cyber-physical system, but also traditional threats (e.g., natural hazards) that will now impact the physical part embedded with emerging technologies that enables the interaction with the cyber part. Therefore, a study, as the one detailed in this research, that provides the theoretical foundation for the analysis of these cyber-physical systems beyond the security domain and by considering civil engineering principles (e.g. fragility functions) is of great necessity.

Currently, there is an increasing research interest related to either the impact (i.e., cyber or physical) of cyber-attacks on the cyber-physical system [39] or the increased complexity due to interdependencies [40]. However, there need to be more studies related to the impact on the robustness level of transportation networks when its integral parts (i.e., IoT-enabled transportation infrastructure) coupled with different levels of cyber-physical interdependencies are subjected to earthquake events. Indeed, many studies and EU projects mainly focus on the impact of cyber-attacks to transportation networks or elements. For example, Laszka et al. [41] studied the impact of traffic signal tampering attacks on traffic congestion. Similarly, EU projects such as CIPSEC [42] focused on developing a security framework that protects the information and operational technology departments of stakeholders in the transportation domain. Other EU projects, such as RESIST [43], focused on the enhancement of resilience of transport operations after extreme events (e.g., man-made incidents, cyber-attacks etc.), availing of recent advances of technology (i.e., robotic damage assessment of tunnels). PRECINCT EU project targets to connect private and public critical infrastructure stakeholders by providing a framework specification for systematic critical infrastructure security and resilience management availing of advanced technologies (e.g., digital twins) [44]. Additionally, current studies on interdependent networks rely on the assumption of a uniform strong interdependency level, that is once a network node fails, its counterpart in the other network fails immediately. However, this assumption is considered unrealistic for cyber-physical systems [45]. Newly created cyber-physical systems may be coupled with weak interdependencies. For example, modern cyber-physical systems have backup units (e.g., battery-based backup power supplies) and emergency management plans that aim to survive nodes in the short-term [46]. Therefore, the elevated strength of interdependency can result in a degraded serviceability level rather than a total failure state of the system. Furthermore, interdependencies are no longer a bidirectional relationship of the same level. For example, physical serviceability may rely on commands of IoT gateway, but IoT-enabled transportation infrastructure may be unable to manage cyber serviceability. Therefore, a one-to-one relationship is not guaranteed and depends upon the type of provided functions from one network to the other. Moreover, studies overlook the engineering aspects of cyber-physical systems that constitute the interdependent networks [47]. For example, transportation infrastructure that is fragile to earthquake events due to its structural design threatens the robustness of transportation networks from a new cyber-physical perspective.

To bridge this gap, we propose a new robustness assessment approach for transportation networks subjected to earthquake events from a cyber-physical perspective based on its civil engineering aspect. In this approach, the physical network includes the IoT-enabled transportation infrastructure, and cyber networks comprise IoT gateway devices. Both are represented in the form of a graph, that due to its advances has been widely used in transportation systems, with a set of nodes (i.e., physical infrastructure, gateway devices) and a set of edges (i.e., interdependency links) [48]. The novelty relies on coupling the physical and cyber network through different cyber-physical interdependency levels that enable the measurement of the combined cyber-physical serviceability level after an earthquake. In this study, we consider the civil engineering aspect of cyber-physical systems vulnerable to earthquake events. We do this by associating the damage states of transportation infrastructure with cyber-physical serviceability levels. Robustness is then measured considering the reduction of the cyber-physical systems' serviceability level. An illustrative transportation network with cyber-physical systems subjected to earthquake events using seismic data (e.g., ground motions) from real-world transportation infrastructure is provided to demonstrate the approach's applicability. A robustness improvement indicator based on attributes of physical and cyber networks is proposed as an improvement strategy to enhance the robustness level. Comparison with existing studies highlights the usefulness of the study. The results are of interest to stakeholders in the transportation domain (i.e., operators, civil and security engineers) indicating that increasing interdependencies between networks subjected to higher ground motions can significantly reduce robustness.

## 2. Related work

A review of related work within the area of robustness of interdependent networks from a cyber-physical perspective is presented in this section. While transportation networks consisted of pure engineering systems susceptible to physical threats, it was until recently that new studies focus on their modern cyber-physical perspective [49]

The transportation domain is one of the main application areas of the IoT technology [50]. Current studies focus on identifying new threats, security issues, etc. [51]. Limited studies have focused on developing assessment approaches (e.g., risk, vulnerability) for the transportation domain from a cyber-physical perspective [11,52,53]. On the contrary the energy sector has attracted more interest relating to the robustness of critical infrastructure (e.g. smart-grids) [54,55]. Existing research on robustness approaches for the transportation domain mainly considers the transportation network as an isolated network, subjected to threats such as targeted attacks [56] or natural hazards [57]. Despite the contribution of these studies in the transportation domain, the increasing integration of IoT technology in transportation networks results in new interdependencies.

Indeed, recent studies highlight the need to examine robustness and resilience of critical infrastructure, due to the interdependencies of physical and cyber systems, when considering new threat scenarios (e.g., cyber-attacks) and traditional hazards (e.g., earthquake events) [58]. Specifically, Zhang et al. [17] provided a detailed review of examining the new cyber, physical and social interdependencies by considering the all of the water, transportation, and cyber infrastructure systems and processes. The need for this study was driven by the transition to more intelligent controls of traditional infrastructure through computing and communication. The authors claim the importance of integrating features of the cyber space (e.g., security breaches) to the resilience of infrastructure as well as and the role of Industry 4.0 for enhancing systems resilience. Although, research studies mainly focus on modern power systems, as a crucial sector for examining resilience from a new cyber-physical perspective [59], other sectors have been recently studied too. For example, Dui et al., [60] proposed a risk model for modern transportation cyber-physical systems, focusing on reliability issues (e.g., time) of supply chain sector in case of emergencies (e.g., floods). The authors assessed the risk (i.e., time loss), by simulating the impact of emergency events to modern transportation cyber-physical systems as a representation of sophisticated integration of networked, intelligent, and digital systems within the transportation domain.

Due to the relatively recent development of cyber-physical systems, few studies have investigated the impact of disasters on cyber-physical systems. As highlighted, the cyber-physical deep coupling requires more research among the interacting cyber and physical parts that could lead to cyber-physical coupling failures when subjected to extreme events [61]. For example this case study focused on the power flow impact due to interaction between the information system and the power system subjected to typhoon disasters [61]. Therefore, it studies the impact of a disaster on the power flow as a result of the deep coupling of cyber and physical parts, differentiating from other studies that mainly focus on the impact due to the failure of the physical part. Similarly, Zhu et al., [62] proposed the cyber-physical resilience modelling for systems interrupted by rainfalls events, by considering the interaction of municipal infrastructure, human individuality, vehicle instrument and network information. Argyriou et al., [63] raise concerns about the impact of natural hazards to the operation of intelligent devices (e.g., IoT devices) and subsequently to the operation of the infrastructure. For example, the authors emphasize hardware damage and loss of performance of IoT devices due to several environmental factors (e.g., overheating due to increasing temperatures), extreme events (e.g., rainfall) or earthquake events. Hardware damage would later degrade the operational level of infrastructure (i.e., in this case study port facilities were considered). As a result, a disastrous event can lead to malfunction of the physical part (e.g., degradation of operational level) due to malfunction of the cyber part, due to the deep coupling of the whole cyber-physical system.

The interdependency of networks has attracted attention recently [64]. Several studies focus on the dynamics of cascading failures due to interdependencies [65]. For example, Cheng et al. [66], under the assumption of one-to-one correspondence (i.e., strong interdependencies), showed that traditional robustness improvement strategies (e.g., protection of high-degree nodes) are less efficient for coupled networks with different characteristics (e.g., topology). The same assumption of one-to-one correspondence that is based on the existence of one interdependency level (i.e., strong interdependency level), which differentiates from our work that considers different levels of cyber-physical interdependencies, has been used in other similar studies related to cascading failures [67–69]. Ji et al. [70] studied the robustness of interdependent networks under random failures, considering strong interdependencies. The approach integrates the relative size of the giant connected component as a measure of robustness, which assumes the largest connected component of the network operates after the disruption. This assumption is impractical in transportation networks, as access to critical facilities after a disruption (e.g., hospital) is overlooked [71].

Recent studies have highlighted the need to incorporate the previously overlooked engineering aspect of cyber-physical systems when studying the interdependency of networks. Specifically, Zhang et al. [47] studied the robustness of interdependent cyber-physical systems based on the principles of giant components. To integrate engineering aspects into their approach, they adopt a flow redistribution model mainly applicable to power networks. Tu et al. [46] considered the engineering aspect and the role of strong-weak interdependencies between the networks. They developed a model applicable to power-grid systems, where different types of nodes (e.g., generator, consumer etc.) generate and consume the power flow. Based on load-capacity models, robustness is then measured as the ratio of served and unserved nodes.

Although related studies contribute to their specific research domain, they have certain limitations. Firstly, there is a lack of approaches for modern transportation networks governed by cyber-physical systems when subjected to natural hazards such as earthquakes. Secondly, the assumption of strong interdependencies has been considered impractical in engineering systems. Engineering systems such as cyber-physical systems rely on backup units and emergency plans that will prevent a total failure. Furthermore, interdependencies aim to increase the serviceability level of these cyber-physical systems by integrating cyberspace into physical space. Therefore, research studies should study the impact on the functioning of the coupled networks (i.e., degraded serviceability level) after a disruptive event (e.g., earthquake), rather than strictly considering its total failure. As a result, the approach of this paper assesses the robustness of a transportation network from a cyber-physical perspective. Specifically, it considers the engineering aspect of the physical and cyber networks (e.g., structural model, gateway devices etc.) and the impact of cyber-physical interdependencies levels on the robustness of transportation network.

## 3. Robustness assessment approach

Transportation networks with the coupled physical network (i.e., hereafter referred to it as Physical network) and cyber network (i.e., hereafter referred to it as Cyber network) include cyber-physical systems subjected to earthquake events. The robustness assessment of such transportation networks requires the completion of certain actions that lead to certain outputs, within steps one to four, as shown in the framework presented in Fig. 2.

Step 1 (i.e., Cyber-physical system division) provides a new approach to divide the cyber-physical system into its two complementary subsystems (i.e., civil engineering system and cyber system) for the first time. Step 1 will enable the identification of coupled parts in the subsystems. Step 2 (i.e., Cyber-physical intendencies assignment) provide more information related to the existence of different interdependency levels between the coupled networks with the cyber physical systems. It aligns with the modern cyber-physical systems perspective (e.g., existence of emergency plans, see Section 1) and differentiates from previous works (i.e., See Section 2) that rely on the assumption that once a node within a network fails its counterpart fails immediately. Step 3 (i.e., i.e., Cyber-physical system serviceability level calculation) is based on existing equations that calculate the operational loss after the removal of a node in a network. Step 4 (i.e., Robustness improvement indicator calculation) is based on our new proposal to integrate an indicator that enables the identification of the pair of interdependent nodes, that their removal will result in greater risk (i.e., greater loss of robustness).

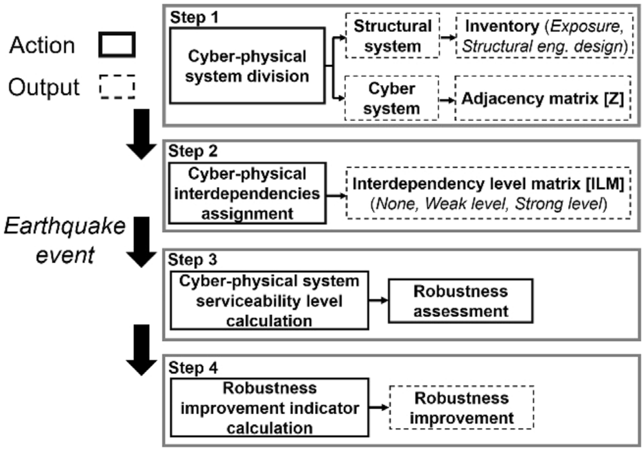
Action
Output
Step 1
Cyber-physical system division
Structural system
Inventory (Exposure, Structural eng. design)
Cyber system
Adjacency matrix [Z]
Step 2
Cyber-physical interdependencies assignment
Interdependency level matrix [ILM]
(None, Weak level, Strong level)
Earthquake event
Step 3
Cyber-physical system serviceability level calculation
Robustness assessment
Step 4
Robustness improvement indicator calculation
Robustness improvement

**Fig. 2.** Robustness assessment framework.

Cyber-physical system division (i.e., Step 1, see Fig. 2) results in the individual study of structural and cyber system. The structural system includes information related to inventory data of transportation infrastructure (i.e., see 3.1.1). Inventory data includes information about the exposure data (location) and structural design details (e.g., typology, fragility functions, etc.) of IoT-enabled transportation infrastructure (e.g., a bridge that is being monitored). The cyber system comprises the interdependency connection between the gateway devices in the Cyber network and the IoT-enabled transportation infrastructure in the Physical network. An adjacency matrix [Z], as shown in Fig. 2, with the discrete values of 0 and 1, represents the presence of an interdependency connection between nodes of two networks. They are represented in the form of dependency links (i.e., connection), indicating that a node of one network (i.e., origin) depends on the function of a node of another network (destination).

### 3.1. Structural system, physical and cyber serviceability levels

The structural system (i.e., output of Step 1, see Fig. 2) includes information related to the physical space (e.g., bridge structure) of the cyber-physical system. Exposure data (i.e., coordinates) of IoT-enabled transportation infrastructure is widely available on public exposure databases (e.g., National Bridge Inventory database (NBI) [72]), as well as open source tools (e.g. Open street map [73]). Structural engineering design details include information related to different typologies of transportation infrastructure (e.g., bridges, roadways etc.) concerning fundamental structural parameters (e.g., type of construction, age of construction, material, etc.). EU projects such as SYNER-G [74] and NBI database [72] identify and groups the main typologies of transportation infrastructure (e.g., bridges, roadways etc.) with respect to specific structural engineering design parameters (e.g., material properties, seismic design level, etc.) Additionally, it provided fragility curves for these specific typologies, necessary to define the damage state. Fragility curves have been widely used to describe the performance of infrastructure at different levels of seismic input intensity measures (e.g., peak ground acceleration (pga)) [75]. The seismicity of a region of interest is based on historical records of earthquake events. The seismic hazard defines the probable level of ground shaking associated with the recurrence of earthquakes in a region. Seismic hazard maps can be either retrieved from national maps (e.g., U.S. Geological Survey [76], SERA [77], OpenQuake [78]), that show the ground motions (i.e., pga) with 2, 5, and 10 % probability of exceedance in 50 years [79],)). Using empirical analytical, expert judgment or hybrid approaches, a fragility curve describes the conditional probability (i.e., the likelihood) of an infrastructure being

**Table 1**
Associated damage states with physical serviceability levels.

| Damage state | Post event physical serviceability level (Traffic flow capacity (%)) |
|---|---|
| No damage, Slight | *Fully serviceable (100 %)* |
| Moderate | *Partially serviceable (50 %–75 %)* |
| Extensive | *Partially serviceable (25 %–50 %)* |
| Complete | *Closed (0 %)* |

damaged beyond a specific damage level, for a given ground motion intensity [80]. Fragility curves are expressed as a lognormal distribution function of two-parameter (i.e., median and standard deviation) [81], as shown in Eq. (1).

$$\mathrm{P}(\mathrm{C}|\mathrm{IM}=x)=\Phi\left(\frac{\ln(\mathrm{x}/\theta)}{\beta}\right) \tag{1}$$

where $\mathrm{P}(\mathrm{C}|\mathrm{IM}=x)$ is the probability that a ground motion with intensity measure (IM) (i.e., IM such as pga), $\mathrm{IM}=x$ will cause the structure to collapse. $\Phi()$ is the standard normal cumulative distribution function (CDF), $\theta$ is the median of the fragility function (i.e., the IM level with 50 % probability of collapse), and $\beta$ is the standard deviation of $\ln$ IM.

There are five main damage states, related to the limits of structural capacity of the infrastructure (e.g., displacement), namely, no damage, slight, moderate, extensive, and complete (i.e., collapse). While post event physical serviceability level (i.e., serviceability level of Physical network after an earthquake), as the residual percentage of traffic flow capacity, are to be determined by operators based on several parameters (e.g., type of failure, detour routes, etc.), empirical studies have associated them with the actual damage state of transportation infrastructure [82,83]. Specifically, quarter-based capacities adopted in this study have been widely employed to associate the damage states with serviceability levels of bridges (i.e., *fully serviceable, partially serviceable, closed*) [84]. For example, a bridge labeled with moderate damages is partially serviceable in an interval of 50 % to 75 % of traffic flow capacity [85]. A bridge that collapses is closed and thus, operates with 0 % of traffic capacity. Table 1 describes the adopted serviceability levels associated with the damage states of a transportation infrastructure.

Similarly, the primary function of an IoT gateway device (i.e., Cyber network) associated with the traffic flow monitoring data, is to manage the sensing networks of IoT-enabled transportation infrastructure. Gateway devices issues (e.g., missing data, hardware malfunction after the event, see Section 1) can result in degraded cyber serviceability levels. Therefore, we consider two post-event cyber serviceability levels for IoT gateway devices, in terms of data processing, namely *fully serviceable* (i.e., 100 %) and *non-serviceable* (i.e., 0 %). Fully serviceable describes the state in which an IoT gateway device can collect the quantity of data in the necessary quality and without hardware failure after the event, to perform management tasks (i.e., control of interconnected sensing network). A non-serviceable gateway device fails to perform management tasks after the earthquake event and results in a degraded physical serviceability level.

### 3.2. *Cyber-physical interdependencies*

Assignment of cyber-physical interdependencies (i.e., Step 2, see Fig. 2) indicates the presence of connection between the coupled networks. Indeed, IoT-enabled transportation infrastructure relies on the interdependencies between the physical and cyber network [86]. Due to the complexity of these systems, elevated levels (e.g., strong) and forms (e.g., bidirectional) of interdependencies have emerged to indicate the strength of their relationship (e.g., weak, strong) (i.e., see Section 1). The specific levels and forms impact the serviceability level of either physical or cyber networks and, subsequently, the robustness of the transportation network. The assignment of a certain level of interdependency between nodes of the physical and cyber network relies on the impact of the functionality of the node of one network when its coupled node in the other network malfunctions (i.e., degraded physical or cyber serviceability level).

The modelling of networks' functional interdependencies necessitates the consideration of assumptions of certain rules that govern the two networks, based on the above assumptions. These rules originate from the new cyber-physical perspective that modern transportation systems operate, as detailed above (see Section 1). In contrast to previous studies (i.e., see Section 2), the new cyber-physical perspective of modern systems is characterized by different interaction among interdependent networks. Specifically, failed nodes in one network will not directly lead to failed nodes in the interacting network (i.e., strong level of interdependency), but will result in indirect effects such as loss of an operational level key feature (e.g., communication efficiency) [45,70]. The so called “weak” interdependency among interacted networks is introduced to characterize the new cyber-physical reality. Although well defined (i.e., weak interdependency), there are still unclear aspects, due to the relatively premature existence of these systems in the transportation domain, that necessitate the consideration of certain assumptions. The first assumption in this study is that we consider the serviceability level, in terms of traffic flow, of a transportation system as the impact area (i.e., indirect effect) of a failed node. Degradation of traffic flow has been well studied as the impact area affected by traditional disastrous events (e.g. earthquake) in transportation systems [87]. As detailed in Section 2, a disastrous event can result in hardware damage or malfunction of the sensing devices that could impact the entire operational level of the physical infrastructure. In this study we consider traffic flow as the key parameter of the serviceability level that is impacted due to the deep coupling of cyber-physical system subjected to a disastrous physical event. We adopt the same levels of post event physical serviceability levels, as detailed in Table 1, that currently describe the correlation of the disastrous event (i.e., earthquake) with a physical infrastructure, without considering the cyber part. Specifically, for this model we assume that the partial serviceability of a physical node due to a failed cyber node will follow the values of Table 1 (i.e., 25 %–75 %) that are the estimated values for post serviceability levels after earthquake events. Due to this theoretical modelling approach and lack of networks that are ubiquitously operating under a cyber-physical perspective, partially serviceability either to a failed physical node or a failed cyber node will adopt the values of Table 1. These values are indicative and can be modified by experts who have a bespoke knowledge of the system operation and needs.

Firstly, we consider three interdependency levels (IL) namely, *None, Weak* and *Strong* associated with the discrete variables of 0, 0.5, and 1. An interdependency level matrix, $\mathrm{ILM}_{\mathrm{C}\to\mathrm{P}}[\mathrm{ILM}_{\mathrm{ni,C},}\ \mathrm{ILM}_{\mathrm{ni,P}}]$ is developed to describe the dependency level of Physical network nodes on Cyber network nodes. Similarly, an interdependency level matrix $\mathrm{ILM}_{\mathrm{P}\to\mathrm{C}}[\mathrm{ILM}_{\mathrm{ni,P},}\ \mathrm{ILM}_{\mathrm{ni,C}}]$ is developed to describe the dependency level of nodes of Cyber network on nodes of Physical network. Routing of data from a physical structure to a gateway device and vice versa indicates an interdependency between the two networks. Cyber-physical interdependencies levels should be assigned by stakeholders who have a bespoke knowledge of their system. Cyber-physical interdependency levels among nodes of coupled networks exist when there is an established communication between them. The established communication relies on data routing, as the process of moving data from one node of one network to another node of the coupled network. Stakeholders involved in the development of the cyber network (e.g., Information Technology staff) have a bespoke knowledge of the data routing of their network. It is the level of communication (cyber-physical interdependencies level) that should be determined based on the impact to the operational loss of one network node (e.g., network 1, node 1) to the dependent network node (e.g., network 2, node 1), after the presence of communication has been identified. Stakeholders involved in the operation of the transportation network (e.g., civil engineers) have a bespoke knowledge of the physical system. Independency levels enable stakeholders to determine the final operational loss of a network node, in the aftermath of a loss of its counterpart. As in the aftermath of a disaster in a transportation network, operational level relies on experts' judgment. As the study of cyber-physical systems in transportation networks is still in its infancy, experts' judgment is mandatory for the assignment of interdependency levels. Specifically, while for civil engineering systems, the operational level can be determined based on the traffic flow, the impact due to malfunction of nodes in the cyber network has yet to be studied. Therefore, the assignment of levels relies on a conventional scale from zero to one as detailed within this section.

The interdependency level assigned as None (0) indicates no relationship between nodes of the Physical and Cyber network in terms of provided data. We define a weak dependency level (i.e., 0.5) of nodes of Cyber network on nodes of Physical network (i.e., $n_{i,P} \rightarrow n_{i,C}$ = weak), if the cyber serviceability level (i.e., IoT gateway devices) is unrelated with the post-event physical serviceability level (see Table 1). A weak level indicates the existence of a relationship between the gateway device (i.e., nodes of Cyber network) and the IoT-enabled transportation infrastructure (i.e., nodes of Physical network), but for data unrelated to traffic flow monitoring data (e.g., environmental conditions of the structure, see Section 1). Therefore, the cyber-serviceability level of the gateway device will not be affected by potential missing values after an earthquake event (see Section 3.1.1). Similarly, we define a strong dependency level (1) of nodes of the Cyber network on nodes of the Physical network (i.e., $n_{i,P} \rightarrow n_{i,C}$ = strong), if the cyber serviceability level is affected by the post-event physical serviceability level. Therefore, the cyber serviceability level will be assigned as non-serviceable (i.e., 0 %), if the evaluation of the damage state of IoT enabled transportation infrastructure is indicated as complete (i.e., collapse), that results in degradation of physical serviceability level to 0 % (see Table 1). We define a weak dependency level of nodes of Physical network on nodes of Cyber network (i.e., $n_{i_c} \rightarrow n_{i,p}$ = weak), if the physical serviceability level of IoT enabled transportation infrastructure depends on commands of the gateway devices, independently of its cyber serviceability level. Similarly, a strong dependency level of nodes of the Physical network on nodes of the Cyber network (i.e., $n_{i_c} \rightarrow n_{i,p}$ = strong), indicate that physical serviceability level relies on commands of gateway devices based on its serviceability level. The distinction between weak and strong levels depends upon the existence of back up plans for missing data, such as prediction of the missing data based on historical data [88]. On the one hand, if a non-serviceable node of the Cyber network can retrieve missing data for the dependent node of the Physical network, the latter can maintain its physical serviceability level. On the other hand, if a non-serviceable node of the Cyber network cannot retrieve missing data for the dependent node of the Physical network, then the physical serviceability level of the latter will be degraded.

Currently, no literature associates a gateway device's malfunction with the level of degradation of the physical serviceability level of transportation infrastructure. Indeed, while IoT applications (e.g., smart traffic lights) with the integration of sensing networks in transportation infrastructure (e.g., road intersections), maximise their serviceability level, they do not consider the impact (e.g., degradation of physical serviceability level) due to *non-serviceable* IoT devices [89]. Degradation of the physical serviceability level due to a *non-serviceable* node of the Cyber network can be determined by stakeholders (i.e., operators, civil and security engineers) who have a bespoke knowledge of their system [90]. In this study, following the rationale of Table 1, we uniformly assume that the physical serviceability level for every node of the Physical network is *partially serviceable*, ranging from 25 % to 75 %, when they strongly depend on a non-serviceable node of the Cyber network.

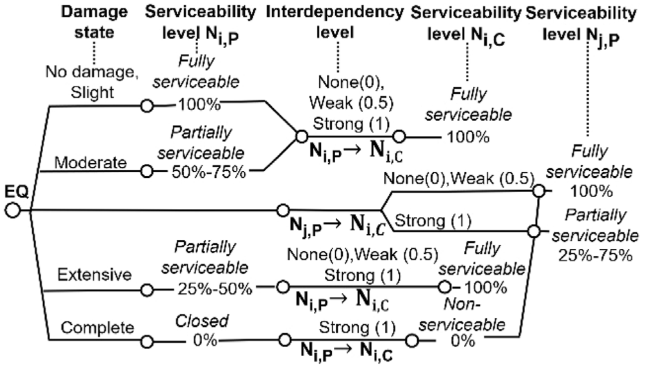
Damage state
Serviceability level $N_{i,P}$
Interdependency level
Serviceability level $N_{i,C}$
Serviceability level $N_{j,P}$
EQ
No damage, Slight
Moderate
Extensive
Complete
Fully serviceable 100%
Partially serviceable 50%-75%
Partially serviceable 25%-50%
Closed 0%
None(0), Weak (0.5) Strong (1)
$N_{i,P} \rightarrow N_{i,C}$
Fully serviceable 100%
$N_{j,P} \rightarrow N_{i,C}$
None(0),Weak (0.5)
Strong (1)
Fully serviceable 100%
Partially serviceable 25%-75%
None(0),Weak (0.5) Strong (1)
$N_{i,P} \rightarrow N_{i,C}$
Fully serviceable 100%
Strong (1)
$N_{i,P} \rightarrow N_{i,C}$
Non-serviceable 0%

**Fig. 3.** Event tree analysis associating damage state, interdependency and serviceability levels of networks.

In this study, Fig. 3 shows, in the form of an event tree, the post-event serviceability levels associated with the damage states and the cyber-physical interdependency levels when considering an earthquake (i.e., EQ) event. For example, after an earthquake event, if a node of the Cyber network (i.e., $n_{i,C}$ strongly depends on a node of the Physical network (i.e., $n_{i,P}$) that is assigned as closed (i.e., complete damage state) then the cyber serviceability level of node $n_{i,C}$ is assigned as non-serviceable (0 %). Therefore, a different node of the physical network (i.e., $n_{j,P}$) that is strongly dependent on the non-serviceable node of the Cyber network (i.e., $n_{i,C}$) will be assigned as partially serviceable (i.e., physical serviceability level ranges to 25 %–75 %). As detailed in Sections 1 & 2, an earthquake event can lead to hardware damages or malfunction of devices that could later impact the physical infrastructure managed by it. In this study, we adopt operational levels as per Table 1 to theoretically deploy our model. As illustrated in Fig. 3, a physical node "physical node i "has failed (i.e., operational level is equal to zero) when the damage state is assigned as complete. In that case, if the linked cyber node "cyber node i " directly fails (i.e., strong interdependency), due to hardware damage or malfunction, then it will impact potential dependent physical node(s) "physical node(s) j" leading to partially serviceability levels, if for example they are coupled by strong interdependency level. For this model we assume that partially serviceability due to a failed cyber node will follow the values of Table 1 (i.e., 25 %–75 %) that are the estimated values for post serviceability levels after earthquake events.

### 3.3. Robustness assessment

The robustness of modern transportation networks, with cyber-physical systems, defines the ability of contributing elements in both the physical and cyber space, to reserve the predesigned serviceability level without significant reduction due to disruption. To represent the performance of the whole transportation network, we consider the performance of the contributing interdependent elements in both spaces. Therefore, the overall cyber-physical system serviceability level is measured by considering the individual physical and cyber serviceability level of contributing nodes in the Physical and Cyber networks, combined with their interdependency levels, as shown in Eq. (2). Robustness is then measured (i.e., Step 3, see Fig. 2) as the loss of the cyber-physical serviceability level, based on Eq. (3).

$$\begin{aligned} \mathrm{CPS-SL} = \sum_{i=1}^{n} (\mathrm{PSL}_{\mathrm{ni,P}} + \mathrm{CSL}_{\mathrm{ni,C}}) \times \mathrm{ILM}_{\mathrm{P \rightarrow C}}\left[\mathrm{ILM}_{\mathrm{ni,P}}, \mathrm{ILM}_{\mathrm{ni,C}}\right] \\ \times \mathrm{ILM}_{\mathrm{C \rightarrow P}}\left[\mathrm{ILM}_{\mathrm{ni,P}}, \mathrm{ILM}_{\mathrm{ni,C}}\right]) \end{aligned} \tag{2}$$

CPS-SL represents the cyber-physical system serviceability level, PSL represents the physical serviceability level that ranges between 0 and 1 (see Table 1). CSL represents the cyber serviceability level that ranges between 0 and 1 (see Fig. 1), and ILM represents the cyber-physical interdependency levels and values that range between 0 and 1 (see Fig. 1).

$$\mathrm{R(G)} = \frac{\mathrm{CPS-SL(G)} - \mathrm{CPS-SL'(G)}}{\mathrm{CPS-SL(G)}} \tag{3}$$

R(G) represents the robustness of the transportation network in the form of a graph G, CPS-SL represents the initial cyber-physical system serviceability level, and CPS-SL' represents the final cyber-physical system serviceability level after the earthquake event. The more robust a cyber-physical system is, the lower the magnitude of the initial loss of cyber-physical serviceability following an earthquake event.

### *3.4. Robustness improvement strategy*

To improve the robustness of modern transportation networks in terms of cyber-physical systems serviceability level (i.e., CPS-SL), we propose the following robustness improvement indicator (RII), as shown in Eq. (4). The RII aims to identify the pair of interdependent nodes, that their removal will result in greater risk (i.e., greater loss of robustness). Therefore, their enhancement, in physical and cyber space, will reduce the proportion of robustness loss. RII combines physical attributes (likelihood) and cyber attributes (i.e., impact) of nodes in the Physical and Cyber network. Specifically, we combine the probability of complete damage, for every node of the physical network (i.e., $n_{i,P}$) that is strongly dependent on nodes of cyber network (i.e., $n_{i,C}$), with the dependency out-degree (i.e., number of external edges) of node $n_{i,C}$, when the latter (i.e. dependency out-degree) is assigned a strong level.

$$\mathrm{RII} = \mathrm{P}_{\mathrm{ni,P}}(\mathrm{Complete}) \times \mathrm{Dout}_{\mathrm{ni,C}},\ \text{for } z_{\mathrm{ij}} = 1 \text{ and } \left[\mathrm{ILM}_{\mathrm{C}\rightarrow\mathrm{P}}\right] = 1 \text{ and } \left[\mathrm{ILM}_{\mathrm{C}\rightarrow\mathrm{P}}\right] = 1 \tag{4}$$

$\mathrm{P}_{\mathrm{ni,A}}(\mathrm{Complete})$ represents the probability of collapse of a node *i* of the Physical network for a certain intensity measure, IM. $\mathrm{Dout}_{\mathrm{ni,C}}$ represents the dependency out-degree as the number of edges (i.e., interdependencies) from nodes of the Cyber network and destined to node(s) of the Physical network, after the removal of the collapsed node of the Physical network. Restrictions require the existence of an interdependency connection (i.e., $a_{ij}$=1), that is labelled as strong (i.e., $[\mathrm{ILM}_{\mathrm{C}\rightarrow\mathrm{P}}]$=1) to measure the number of nodes $n_{j,\,P}$ that will be affected (i.e., $[\mathrm{ILM}_{\mathrm{P}\rightarrow\mathrm{C}}]$=1) by the degraded serviceability level of node $n_{i,C}$. In practice, it combines the likelihood of failure of a contributing physical element and the cyber impact of a contributing cyber element. After identifying a pair of interdependent nodes, robustness from an engineering perspective includes individual or combined enhancement of the structural system (i.e., see Fig. 2) in physical space and/or the enhancement of cyber systems in cyber space. Specifically, strategies in the physical space are based on retrofit strategies (e.g., energy dissipation devices, structural strengthening strategies, etc.) that improve the performance of the structural system (i.e., Complete damage state probabilities reduced) [91,92]. Strategies in the cyber space are based on missing data techniques (e.g., algorithms) that improve the performance of the cyber system [93] and subsequently reduce the dependency level from strong to weak by maintaining the interdependency connection (see Section 3.2).

## 4. Case study

A cyber-physical transportation network case study is employed to demonstrate the applicability of the robustness assessment approach. We highlight the approach's usefulness by comparing the results with other studies (i.e., see Section 5). The illustrative transportation network employed in previous studies [52] operates under the integration of a physical network and a cyber network represented using graphs G, as shown in Fig. 4. The topology of the physical network (i.e., Physical network) is in the form of an undirected graph G(P), with a set of eight nodes (i.e., $N_{i,P}$ = 8) that represent the IoT-enabled transportation infrastructure, internally connected with fourteen edges. Three IoT gateway devices (i.e., $G_1$, $G_2$, $G_3$), represented as nodes (i.e., $N_{i,C}$ = 3) constitute the topology of the cyber network. The adjacency matrix indicates the existence of interdependencies between the Physical and Cyber networks, as shown in Table 2. The two networks are coupled, under different cyber-physical interdependency levels (i.e., [ILM], see Fig. 2), as shown in Table 3.4. For example, there is an interdependency connection between $G_2$ and $N_8$ (i.e., Z[8,2]=1). Furthermore, the dependency level of $G_2$ on $N_8$ is labelled as weak (i.e., $\mathrm{ILM}_{\mathrm{P}\rightarrow\mathrm{C}}[2,8]$=0.5) and the dependency level of $N_8$ on $G_2$ is labelled as weak ($\mathrm{ILM}_{\mathrm{C}\rightarrow\mathrm{P}}[8,2] = 0.5$).

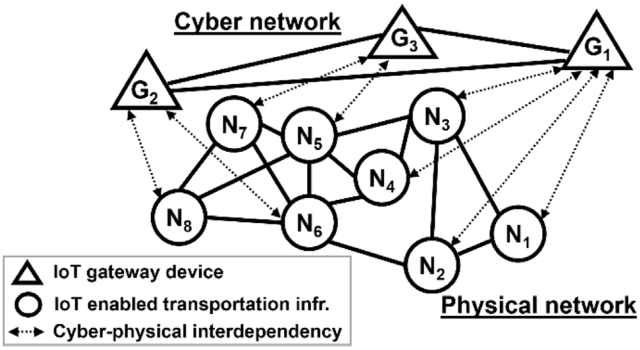

**Fig. 4.** Transportation network case study with the interdependent Physical and Cyber network.

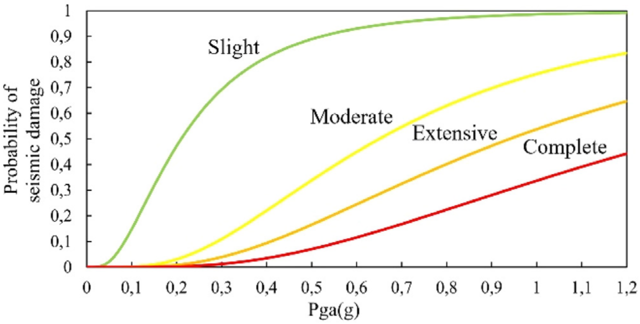

**Fig. 5.** Fragility curve for MSSS concrete typology (Nodes 2,3,4,5,6) [94].

**Table 2**
Adjacency matrix Z for the Physical and Cyber networks.

$$[Z] = \begin{array}{cccc} \mathbf{G1} & \mathbf{G2} & \mathbf{G3} & \\ 1 & 0 & 0 & \mathbf{N1} \\ 1 & 0 & 0 & \mathbf{N2} \\ 1 & 0 & 0 & \mathbf{N3} \\ 1 & 0 & 0 & \mathbf{N4} \\ 0 & 0 & 1 & \mathbf{N5} \\ 0 & 1 & 0 & \mathbf{N6} \\ 0 & 0 & 1 & \mathbf{N7} \\ 0 & 1 & 0 & \mathbf{N8} \end{array}$$

The main transportation infrastructure typologies adopted in this illustrative case study are based on the bridge inventory data by National Bridge Inventory database [72]. Research studies have provided a fragility analysis for several typologies of bridges in Central and Southeastern United States to examine the effectiveness of seismic retrofitting strategies [94,95]. Two of them that constitute 28.9 % of the total inventory (i.e., more than one hundred thousand bridges) are the multi-span supported concrete girder bridges (MSSS concrete) and the multi-span continuous steel girder bridges (MSC steel). Peak ground acceleration was used as the intensity measure (IM). Table 5 provides the details related to the median (i.e., $\theta$) and standard deviation (i.e., $\beta$) (see Eq. (1)) by fragility analysis for the MSSS concrete typology that represents Nodes 2,3,4,5,6 of the Physical network. Similarly, Table 6 provides the details related to median and standard deviation by fragility analysis for the MSC steel typology representing Nodes 1,7,8, of the Physical network. Fig. 5 shows a fragility curve with the damage states for the MSSS concrete typology based on the parameters of Table 5.

### *4.1. Simulations*

A seismic hazard map for the Central and Southeastern United States regions is adopted here [95]. The seismic hazard map indicates the pga

**Table 3**
Interdependency level matrix $[ILM_{P\rightarrow C}]$, indicating the level of dependency of the Cyber network on the Physical network.

$$[ILM_{P\rightarrow C}] = \begin{bmatrix} \mathit{strong}\ (1) & 0 & 0 \\ \mathit{weak}\ (0.5) & 0 & 0 \\ 0.5 & 0 & 0 \\ 0.5 & 0 & 0 \\ None(0) & 0 & 0.5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0.5 & 0 \end{bmatrix}$$

**Table 4**
Interdependency level matrix $[ILM_{C\rightarrow P}]$, indicating the level of dependency of the Physical network on the Cyber network.

$$[ILM_{C\rightarrow P}] = \begin{bmatrix} 0.5 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0.5 & 0 \end{bmatrix}$$

**Table 5**
MSSS concrete typology fragility parameters for Nodes 2,3,4,5,6 of Physical network.

| MSSS concrete Condition | Slight | | Moderate | | Extensive | | Complete | |
|---|---|---|---|---|---|---|---|---|
| | Median | Std | Median | Std | Median | Std | Median | Std |
| As built | 0.21 | 0.71 | 0.65 | 0.63 | 0.94 | 0.65 | 1.32 | 0.66 |

**Table 6**
MSC steel typology fragility parameters for nodes 1,7,8 of Physical network.

| MSC steel Condition | Slight | | Moderate | | Extensive | | Complete | |
|---|---|---|---|---|---|---|---|---|
| | Median | Std | Median | Std | Median | Std | Median | Std |
| As built | 0.19 | 0.56 | 0.36 | 0.54 | 0.44 | 0.56 | 0.57 | 0.59 |

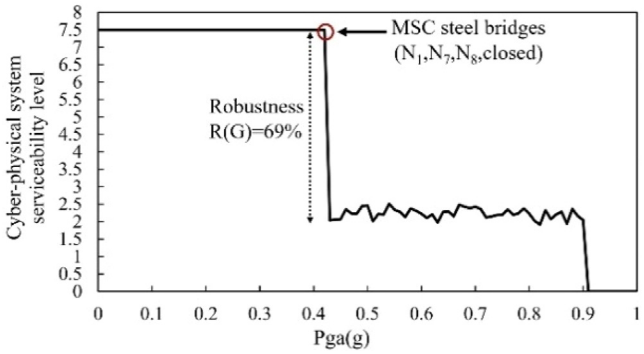

**Fig. 6.** Cyber-physical system serviceability level and robustness assessment of transportation network case study.

(i.e., IM) for probability of exceedance 7 % in 75-year hazard. For purposes of demonstration of the transportation network robustness assessment approach, we consider that all nodes of the Physical network experience the same ground motion. Results of robustness assessment approach based on Eqs. (2) & (3) and Fig. 3 for the considered bridge inventory (i.e., Tables 2, 3, 4, 5, 6) are shown in Fig. 6. Simulations are performed using a uniform random number generator [96], to determine the traffic flow capacity of nodes of the Physical network associated with different damage states and cyber-physical interdependency levels based on the experienced ground motion (i.e., see Table 1 and Fig. 3).

**Table 7**
Robustness improvement indicator in descending order for every pair of nodes of transportation network case study.

| DS Nodes | Complete damage state $(N_1,N_7,N_8)$ [calculated using EQ4] | Complete damage state $(N_2,N_3,N_4,N_5,N_6)$ [calculated using EQ4] |
|---|---|---|
| Node 1 | $RII = P_{ni,P}(\text{Complete}) \times Dout_{ni,C}$<br>RII(1)=0.32×3 = 0.96 | RII(1)=0.79×3 = 2.37 |
| Node 7 | RII(7)=0.32×1 = 0.32 | RII(7)=0.79×1 = 0.79 |
| Node 2 | RII(2)=0.04×0 = 0 | RII(2)=0.04×0 = 0 |
| Node 3 | RII(3)=0.04×0 = 0 | RII(3)=0.04×0 = 0 |
| Node 4 | RII(4)=0.04×0 = 0 | RII(4)=0.04×0 = 0 |
| Node 5 | RII(5)=0.04×0 = 0 | RII(5)=0.04×0 = 0 |
| Node 6 | RII(6)=0.04×0 = 0 | RII(6)=0.04×0 = 0 |
| Node 8 | RII(8)=0.32×0 = 0 | RII(8)=0.32×0 = 0 |

In this example, as a first step nodes $N_1$, $N_7$, $N_8$ are initially removed from the graph (i.e., complete damage state for pga =0.43g as can be seen in Fig. 6) and thus are labelled as *closed* (i.e., 0 %, see Table 1). As described above, for the purposes of demonstration and simplicity we assume that every physical node experiences the same ground motion. Therefore, nodes $N_1$, $N_7$, $N_8$ are the first nodes that exceed the capacity level and for a ground motion equal to 0.43 their damage state is assigned as complete. Nodes $N_1$, $N_7$, $N_8$ adopts the parameters of the MSC steel typology (i.e., see Table 6) with median value equal to 0.57. Due to the lower median value of $N_1$, $N_7$, $N_8$ (see Table 6) in comparison to the Nodes 2,3,4,5,6 that follows the MSSS concrete typology (i.e., see Table 5) with median value equal to 1.32, the nodes $N_1$, $N_7$, $N_8$ primarily exceeds the probability of complete damage state due to the considered ground motion (i.e., pga equal to 0.43). In step two we consider the level of interdependencies (i.e., none, weak, strong) among the interacting physical and cyber nodes. The existence of strong dependencies between $N_1$ and $G_1$ (i.e., $N_1 \rightarrow G_1$=strong, see Table 3) and between $N_7$ and $G_3$ (i.e., $N_7 \rightarrow G_3$=strong, see Table 3) means the cyber serviceability level of the gateways reduce (i.e., $G_1$ & $G_3$) to become *non-serviceable* (i.e., 0 %) (see Fig. 3). In step three we consider the level of interdependencies (i.e., none, weak, strong) among failed cyber nodes and physical nodes. Therefore, the existence of strong interdependencies between $G_1$ and $N_1$, $N_3$ & $N_4$ (i.e., $G_1 \rightarrow N_1$, $N_3$, $N_4$ = strong, see Table 4) the physical serviceability level of $N_1$, $N_3$& $N_4$ reduces to become *partially serviceable* (i.e., 25 %–75 %, see Fig. 3). Similarly, the existence of strong interdependencies between $G_3$ and $N_5$ (i.e., $G_3 \rightarrow N_5$ = strong, see Table 4) reduces the physical serviceability level of $N_5$ to become *partially serviceable* (i.e., 25 %–75 %, see Fig. 3). Despite node $N_8$ being removed from the graph, only the physical serviceability level is impacted (i.e., *closed* 0 %). The existence of weak interdependencies with $G_2$ (i.e., $N_8 \rightarrow G_2$=weak) does not impact the cyber serviceability level of the latter (i.e., *fully serviceable* (100 %). As a result, the initial removal of nodes $N_1$, $N_7$, $N_8$ with their associated cyber-physical interdependencies with $G_1$, $G_2$, $G_3$ results in a reduction of cyber-physical serviceability level (see Eq. (2)) of 69 % (i.e., robustness R(G), see Eq. (3)). The cyber-physical serviceability level is completely reduced (i.e., R(G)=100 %) after the removal of Nodes 2,3,4,5,6 (i.e., pga=0.91g, see Fig. 6).

### *4.1.1. Robustness improvement indicator*

The robustness improvement indicator (RII) aims to improve the cyber-physical serviceability level of interdependent pair of nodes, considering attributes of the physical and cyber space (see Eq. (4)). We rank the nodes in a descending order of prioritization as shown in Table 7. The results indicate that node $N_1$ has the greatest RII (i.e., RII(1)=0.96 when the damage state of $N_1$,$N_7$,$N_8$ is labelled as complete P(complete)=0.32, and RII(1)=2.37 when the damage state of $N_2$,$N_3$,$N_4$,$N_5$,$N_6$ is labelled as complete P(complete)=0.79. The greater RII indicates that improvement strategies should be undertaken in the interdependent pair of nodes that include $N_1$.

Based on the results of Table 7, we reassess the robustness of the transportation network case study after the retrofit of node $N_1$ (i.e., MSC steel bridge typology) based on the fragility analysis parameters,

**Table 8**
Retrofit MSC steel typology fragility parameters for nodes 1,7,8 of Physical network.

| MSC steel Condition | Slight | | Moderate | | Extensive | | Complete | |
|---|---|---|---|---|---|---|---|---|
| | Med | Std | Med | Std | Med | Std | Med | Std |
| Retrofit | 0.26 | 0.72 | 0.43 | 0.70 | 0.56 | 0.71 | 0.92 | 0.73 |

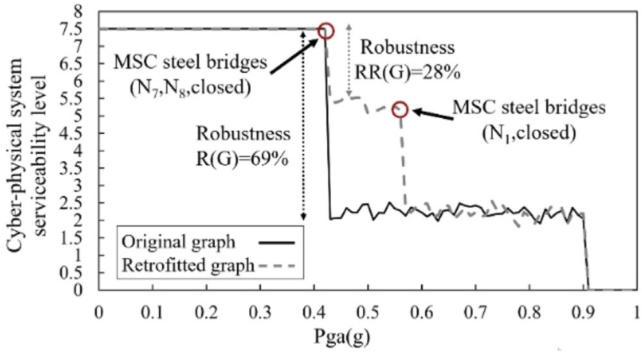

**Fig. 7.** Cyber-physical system serviceability level and robustness assessment of retrofitted transportation network case study.

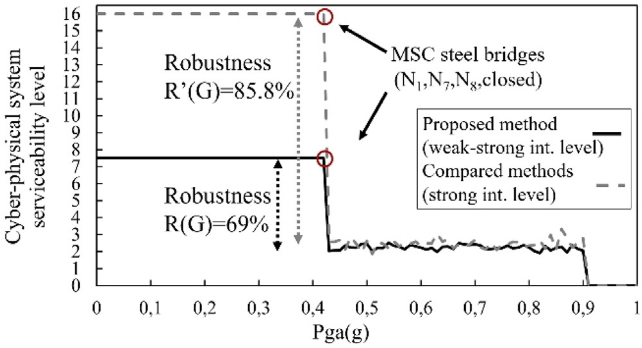

**Fig. 8.** Comparison of proposed robustness approach with existing methods that consider only strong interdependencies.

as shown in Table 8. Fig. 7 displays the results of the transportation network case study. The retrofit strategy of the structural system is selected to improve its performance. Specifically, seismic isolation through elastomeric bearings was a beneficial strategy for reducing the seismic risk for this typology [94,95].

Specifically, strategies in physical space are based on retrofit strategies (e.g., structural strengthening or energy dissipation devices added) that improve the performance of the structural system (i.e., Complete damage state probabilities reduced). Results indicate that the retrofitted transportation network case study is more robust (i.e., an increase of 41 %, from R(G)=69 % to RR(G)=28 %) as it reserves its cyber-physical serviceability level after the retrofit of $N_1$.

### 4.2. Comparison with existing methods

The main assumption of previous studies related to interdependent networks is the existence of purely strong interdependencies between the nodes of networks [67–69]. That is, once a node fails its counterpart fails immediately and completely. Fig. 8 shows the results when we consider the existence of strictly strong interdependencies between the two networks. Specifically, in comparison to the existing assessment of the robustness of the transportation network case study (i.e., R(G), see Fig. 6), we consider a strong interdependency between $N_8$ and $G_2$ (i.e., see Table 3). Therefore, after the removal of $N_8$, the cyber-serviceability level of $G_2$ will become *non-serviceable* (0 %). Results, as displayed in Fig. 8, indicate a significant differentiation in the cyber-physical serviceability levels and subsequently in robustness level when comparing the proposed method with existing methods that consider only one level of interdependencies (i.e., strong). Specifically, the transportation network case study has a lower loss of cyber-physical serviceability level and therefore is more robust when we apply our method, in comparison to existing methods that results indicate that they underestimate the robustness level of transportation network (i.e., 16.8 % increase to robustness level, from R(G)=69 % to R'(G)=85.8 %).

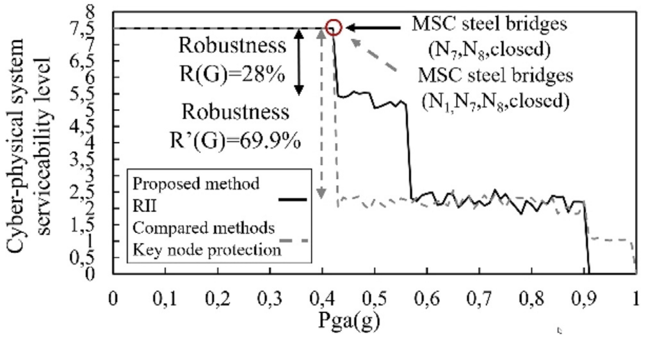

**Fig. 9.** Comparison of proposed robustness improvement strategy with key node protection strategies.

Furthermore, we compare the proposed RII with existing transportation networks' robustness strategies, as discussed in Section 2. One of transportation networks' main robustness improvement strategies is related to key node protection. Key node protection strategies are related to the identification of key nodes based on the main centrality measures (e.g., node degree, node betweenness) [45]). According to these indicators, nodes with a higher number of edges connected to them (i.e., node degree) and nodes that lies more frequently on paths between other nodes acting as a mediator (i.e., node betweenness) have a greater contribution to the robustness level. Although these methods are valuable when considering an isolated network or interdependent networks based on strong interdependencies, they are impractical when considering different interdependency levels based on civil engineering aspects. In the case study, Node 6 has the greatest node degree (i.e., 5) and the greatest betweenness level (i.e., 10). We assess the robustness of the transportation network case study, considering a retrofitted Node 6 (i.e., key node protection). Compared to our proposed method, $N_1$ was determined as the potential retrofitted node based on RII (see Table 5). Results, as shown in Fig. 9, indicate that the transportation network case study has a lower loss of its cyber-physical serviceability level and therefore is more robust when applying our method (i.e., RII) than existing methods (i.e., key node protection). Specifically, the robustness of the transportation networks case study is increased by 41.9 % by adopting our improvement strategy (i.e., R(G)=28 % compared to R'(G)=69.9 %).

## 5. Discussion

Robustness assessment of modern transportation networks necessitates the consideration of a cyber-physical perspective (see Section 1). As integral parts of transportation networks, IoT-enabled transportation infrastructure operates as hybrid engineering systems with different levels of interdependencies between its cyber and physical entities. Despite their transition to cyber-physical systems, traditional hazards (e.g., earthquakes) threaten the robustness of a transportation network that relies on its operation from both the physical and cyber serviceability levels.

Functional interdependencies between the cyber and physical space necessitate a new robustness assessment approach to transportation networks under a cyber-physical perspective (see Section 1). Results from our research indicate that due to the existence of interdependencies (i.e., weak, strong), where nodes of one network can manage nodes of another network, transportation network can suffer significant loss of its cyber-physical serviceability level and be less robust (i.e., R(G)=69 %, see Fig. 6). Thus, we proposed an RII based on physical attributes (i.e., probability of collapse due to ground motions) and cyber attributes (i.e., interdependency-out-degree). RII enables stakeholders to identify pairs of nodes, their enhancement could result in reduced loss of cyber-physical serviceability level and be a more robust system. Application of RII increased the robustness of the transportation network (i.e., 41 % increase of robustness, see Fig. 7).

Existing robustness methods either build on the assumption of a one-to-one correspondence or overlook the civil engineering aspects of cyber-physical systems, reducing their accuracy. To highlight the usefulness of our approach, we compared our approach with the existing methods. Results differentiate when we strictly consider strong interdependencies compared to different levels of interdependencies. Specifically, the robustness of the transportation networks case study is underestimated when adopting existing methods compared to our approach (i.e., 16.8 % increase of robustness, see Fig. 8). IoT-enabled transportation infrastructure relies on integrating cyber and physical space, but a failure of one space does not necessarily result in a failure of its counterpart but rather a degradation of its serviceability level. Furthermore, existing robustness improvement strategies are based on the key node protection strategy that avails of advancements in graph theory and centrality measures (e.g., node degree). Although these strategies may be useful when considering only the physical network that bases its operation on topological attributes, it is impractical when considering interdependent physical and cyber networks. A comparison between our approach and existing improvement strategies highlights differences. Specifically, application of the RII results in lower loss of cyber-physical serviceability levels and therefore a more robust system when compared to key node protection strategies (i.e., 41.9 % increase of robustness, see Fig. 9).

Despite the contribution of this paper, it comes with certain challenges that stakeholders (i.e., operators, civil and security engineers) should address. Challenges are mainly based on the emerging research domain of different levels of interdependencies. Integrating the cyber space with the physical space by implementing advanced technology (e.g., IoT) in transportation infrastructure necessitates further collaboration between civil and security engineers that has yet to be established [97]. This challenge increases when considering that the transportation domain is the backbone of modern societies. Serviceability levels and interdependency levels should be collaboratively assigned by stakeholders who as experts have a bespoke knowledge of their system. Although data related to civil engineering sub-systems (e.g., parameters for fragility functions) have been validated and therefore demonstrate the real-world applicability of the approach, this is not always the case for data related to the security domain. The premature level of research for real-world transportation infrastructure that operates as cyber-physical systems in transportation networks has resulted in a lack of data for their operational behavior. Therefore, the impact of operational loss of a cyber network node to its coupled physical network node has not yet been studied. While the scope of the paper is to highlight the existence of different interdependency levels between cyber and physical networks, that affect the robustness of modern transportation networks, it adopts a rather conventional approach when such levels should be quantified, that relies on a quantified scale from zero to one. Further evaluation of the impact to the operational level of cyber network nodes to physical network nodes and vice versa, will complement the role of experts in the assignment of interdependency levels. The illustrative network adopted in the case study (i.e., see Section 4), enables the demonstration of the applicability and usefulness of the approach. The challenges related to a real-world example mainly rely on computational resources due to the large amounts of data, security sensitivity of data, etc., while it will not affect the applicability of the approach. Specifically, data related to the structural system (i.e., fragility functions parameter) are widely available for different types of transportation infrastructure, while data related to cyber network should be also assigned based on experts' judgment due to the lack of published data.

Analysis of critical infrastructure systems from a new cyber-physical perspective is still in its relative infancy. Currently, analysis of cyber-physical systems that operate in transportation domain, can be found in smart city applications, with the variety of them focusing on connected and automated vehicles [98]. Other applications relate to the development of emergency management systems [99] and supply chain optimization [100], that rely on highly interacting edge computing cyber-physical systems embedded in transportation infrastructure (e.g., roads, bridges etc.). The proposed approach as detailed in previous sections, takes a step further these applications, as it introduces the role of natural hazards in relation to the operation of the entire cyber-physical system. Therefore, malfunction of critical parts operating in cyber space should not only be related to security threats (e.g., Denial of Services attacks) but also to natural hazards, and the impact on the operation of the cyber-physical system should be further investigated. This can be materialized by identifying the physical parts that are susceptible to natural hazards and investigating the level of interdependencies with the cyber parts. The proposed approach provides many potentials to applications that examine the new cyber-physical reality of critical infrastructure. The proposed approach can enrich information regarding the robustness of critical infrastructure that serves as cyber-physical systems, by considering the unique characteristics of the physical parts in terms of structural design and assessing the level of interaction among cyber and physical parts. Expert judgment is of crucial importance as they have a bespoke knowledge of their systems. More specifically, port facilities as analyzed in previous studies [63], include interacting components that operate in physical space (e.g., waterfront) and in cyber space (e.g., edge devices). Such physical components are quite susceptible to natural hazards (e.g., flood, earthquake etc.). Fragility functions can be employed for these structures, given earthquake scenarios based on the seismicity levels of the area of interest [101]. Damage states for the structures of interest and interdependencies among physical and cyber components, based on expert judgment can later define the operational level of cyber spaces and the overall operation levels of the entire cyber-physical system. As research related to damage states, based on fragility functions or other methods, given different hazard scenarios for different structures is extended, more details can be integrated into this approach [102].

## 6. Conclusion

Transportation networks are of vital importance for societies' functioning. Integrating cyber space with physical space has boosted the performance of transportation infrastructure. However, this integration and transition to cyber-physical systems has resulted in increasing complex interdependencies that threaten the robustness of transportation networks to hazards and threats. Current studies focusing on interdependent networks mainly rely on the assumption of strong interdependencies and overlook the engineering aspect of cyber-physical systems. A new robustness assessment approach for transportation networks under a cyber-physical perspective is proposed to bridge this gap. The novel approach considers different levels of interdependencies associated with the damage states and serviceability levels of the coupled physical and cyber network when the former is subjected to earthquake events. Robustness is then measured considering the contributing pair of nodes in the physical and cyber network as the degradation of the overall serviceability level. A new robustness improvements indicator is proposed that is based on physical and cyber attributes. The robustness improvement indicator aims to identify pairs of nodes so that their enhancement can result in more robust systems. A case study of an illustrative transportation network using seismic data from real-world transportation infrastructure is adopted to showcase the application of the approach. Results indicate that transportation networks are less robust to earthquake events due to cyber-physical interdependency levels. Application of robustness improvement indicator resulted in an increase of robustness level by 41 %. To demonstrate the approach's usefulness, we compared the results with existing methods that greatly differentiate. Adopting our proposed improvement strategy results in a 41.9 % increase in robustness. Overall, it has been demonstrated that the proposed robustness assessment approach for transportation networks under a cyber-physical perspective can constitute a valuable method for stakeholders who attempt to integrate the cyber domain into the transportation domain.

## Relevance to resilience

In this study, we focus on robustness as a fundamental aspect of infrastructure resilience, ensuring that systems can withstand and perform effectively under various stresses, shocks, and disruptions. By enhancing robustness, infrastructure becomes more resilient, minimizing downtime, reducing repair costs, and improving public safety during crises. We consider the performance of the system from a new cyber-physical perspective, that can help stakeholders more efficiently improve resilience strategies by combining traditional hazards (e.g., natural hazards) with security issues of emerging technologies in critical infrastructure.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## CRediT authorship contribution statement

**Konstantinos Ntafloukas:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Liliana Pasquale:** Writing – review & editing, Validation, Supervision, Resources, Project administration, Investigation, Funding acquisition, Formal analysis, Conceptualization. **Beatriz Martinez-Pastor:** Writing – review & editing. **Daniel P. McCrum:** Writing – review & editing, Validation, Resources, Project administration, Investigation, Funding acquisition, Formal analysis, Conceptualization.

## Acknowledgments

This work is financially supported by a University College Dublin Advanced PhD Scholarship Scheme 41063.

## References

[1] Ding R, Ujang N, bin Hamid H, Abd Manan MS, Li R, Wu J. Heuristic urban transportation network design method, a multilayer coevolution approach. Physica A: Stat Mech Appl 2017;479:71–83.
[2] Cats O, Jenelius E. Planning for the unexpected: the value of reserve capacity for public transport network robustness. Transport Res Part A: Policy Pract 2015;81:47–61.
[3] Salomon J, Behrensdorf J, Winnewisser N, Broggi M, Beer M. Multidimensional resilience decision-making for complex and substructured systems. Resilient Cities Struct 2022;1:61–78.
[4] Loukas G. Cyber-physical attacks: a growing invisible threat. Butterworth-Heinemann; 2015.
[5] Zhang N, Alipour A. Multi-scale robustness model for highway networks under flood events. Transport Res Part D: Transport Environ 2020;83:102281.
[6] Szyliowicz J, Zamparini L. Freight transport security and the robustness of global supply chains. Transp Rev 2022;42:717–24.
[7] Capacci L, Biondini F, Frangopol DM. Resilience of aging structures and infrastructure systems with emphasis on seismic resilience of bridges and road networks. Resilient Cities Struct 2022;1:23–41.
[8] Fioklou A, Alipour A. Probability of failure estimation for highway bridges under combined effects of uncorrelated multiple hazards. Resilient Cities Struct 2022;1:79–93.
[9] Ntafloukas K, Pasquale L, Martinez-Pastor B, McCrum DP. Identification of vulnerable iot enabled transportation infrastructure into a cyber-physical transportation network. 2023 IEEE International Conference on Cyber Security and Resilience (CSR); 2023.
[10] Liveri D, Theocharidou M, Naydenov R. Railway cybersecurity: security measures in the railway transport sector. ENISA; 2020.
[11] Ntafloukas K, McCrum DP, Pasquale L. A cyber-physical risk assessment approach for internet of things enabled transportation infrastructure. Appl Sci 2022;12:9241.
[12] Ntafloukas K, McCrum DP, Pasquale L. A risk assessment approach for IoT enabled transportation infrastructure subjected to cyber-physical attacks. 32nd European Safety and Reliability Conference Ireland; 2022.
[13] Mishra M, Lourenço PB, Ramana GV. Structural health monitoring of civil engineering structures by using the internet of things: a review. J Build Eng 2022;48:103954.
[14] Putra AS, Warnars HLHS. Intelligent traffic monitoring system (ITMS) for smart city based on IoT monitoring. 2018 Indonesian Association for Pattern Recognition International Conference (INAPR). IEEE; 2018.
[15] Zheng X, Pan L, Chen H, Wang P. Investigating security vulnerabilities in modern vehicle systems. International Conference on Applications and Techniques in Information Security. Springer; 2016.
[16] Gupta M, Benson J, Patwa F, Sandhu R. Secure V2V and V2I communication in intelligent transportation using cloudlets. IEEE Trans Serv Comput 2020;15:1912–25.
[17] Mohebbi S, Zhang Q, Wells EC, Zhao T, Nguyen H, Li M, Abdel-Mottaleb N, Uddin S, Lu Q, Wakhungu MJ. Cyber-physical-social interdependencies and organizational resilience: a review of water, transportation, and cyber infrastructure systems and processes. Sustain Cities Soc 2020;62:102327.
[18] Marashi K, Sarvestani SS, Hurson AR. Identification of interdependencies and prediction of fault propagation for cyber–physical systems. Reliab Eng Syst Saf 2021;215:107787.
[19] Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: current status, challenges and prospective measures. 2015 10th international conference for internet technology and secured transactions (ICITST). IEEE; 2015.
[20] Zanzi L, Cirillo F, Sciancalepore V, Giust F, Costa-Perez X, Mangiante S, Klas G. Evolving multi-access edge computing to support enhanced IoT deployments. IEEE Commun Stand Mag 2019;3:26–34.
[21] Aazam M, Huh E-N. Fog computing and smart gateway based communication for cloud of things. 2014 International conference on future internet of things and cloud. IEEE; 2014.
[22] Bansal S, Kumar D. IoT ecosystem: a survey on devices, gateways, operating systems, middleware and communication. Int J Wirel Inf Netw 2020;27:340–64.
[23] Haghi M, Neubert S, Geissler A, Fleischer H, Stoll N, Stoll R, Thurow K. A flexible and pervasive IoT-based healthcare platform for physiological and environmental parameters monitoring. IEEE Internet Things J 2020;7:5628–47.
[24] Ooi B-Y, Kong Z-W, Lee W-K, Liew S-Y, Shirmohammadi S. A collaborative IoT–gateway architecture for reliable and cost effective measurements. IEEE Instrum Meas Mag 2019;22:11–17.
[25] Tung NT, Phong NH, Huy TLD, Huy NM, Tuyen ND, Phuong LM. Development and performance analysis of intelligent street lighting for smart cities using LoRa Wan. Eng Technol 2020;2:1.
[26] Brincat AA, Pacifici F, Martinaglia S, Mazzola F. The internet of things for intelligent transportation systems in real smart cities scenarios. 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE; 2019.
[27] Hu Z, Tang H. Design and implementation of intelligent vehicle control system based on internet of things and intelligent transportation. Sci Program 2022;2022:1–11.
[28] Martinez-Pastor B, Nogal M, O'Connor A, Teixeira R. Identifying critical and vulnerable links: a new approach using the Fisher information matrix. Int J Crit Infrastruct Protect 2022;39:100570.
[29] Decò A, Frangopol DM. Life-cycle risk assessment of spatially distributed aging bridges under seismic and traffic hazards. Earthq Spectra 2013;29:127–53.
[30] Akiyama M, Frangopol DM, Ishibashi H. Toward life-cycle reliability-, risk-and resilience-based design and assessment of bridges and bridge networks under independent and interacting hazards: emphasis on earthquake, tsunami and corrosion. Struct Infrastruct Eng 2020;16:26–50.
[31] Alipour A, Shafei B. An overarching framework to assess the life-time resilience of deteriorating transportation networks in seismic-prone regions. Resilient Cities Struct 2022;1:87–96.
[32] Arthurs P, Gillam L, Krause P, Wang N, Halder K, Mouzakitis A. A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles. IEEE Trans Intell Transport Syst 2021.
[33] Al-Osta M, Bali A, Gherbi A. Event driven and semantic based approach for data processing on IoT gateway devices. J Ambient Intell Humaniz Comput 2019;10:4663–78.
[34] França CM, Couto RS, Velloso PB. Missing data imputation in Internet of Things gateways. Information 2021;12:425.
[35] Spencer BF, Jo H, Mechitov KA, Li J, Sim S-H, Kim RE, Cho S, Linderman LE, Moinzadeh P, Giles RK. Recent advances in wireless smart sensors for multi-scale monitoring and control of civil infrastructure. J Civ Struct Health Monit 2016;6:17–41.
[36] Cheng Q, Liao W, Fei Y, Tian Y, Lu X, Zhang W, Ghahari F, Kurtulus A, Taciroglu E. A cost-benefit analysis of sensor quality and spatial density for rapid regional post-event seismic damage assessment: application to Istanbul. Soil Dyn Earthq Eng 2022;163:107495.
[37] Marchang J, Sanders B, Joy D. Adaptive V2V routing with RSUs and gateway support to enhance network performance in VANET. In: Wired/Wireless Internet Communications: 16th IFIP WG 6.2 International Conference, WWIC 2018, Boston, MA, USA. Springer; 2018. June 18–20Proceedings. 2018.
[38] Pal K, Shakshuki E. Supply chain transport management, use of electric vehicles, review of security and privacy for cyber-physical transportation ecosystem and related solutions. Procedia Comput Sci 2024;238:135–42.

[39] Humayed A, Lin J, Li F, Luo B. Cyber-physical systems security—a survey. IEEE Internet Things J 2017;4:1802–31.
[40] Sturaro A, Silvestri S, Conti M, Das SK. A realistic model for failure propagation in interdependent cyber-physical systems. IEEE Trans Netw Sci Eng 2018;7:817–31.
[41] Laszka A, Potteiger B, Vorobeychik Y, Amin S, Koutsoukos X. Vulnerability of transportation networks to traffic-signal tampering. In: 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS). IEEE; 2016. p. 1–10.
[42] Enhancing critical infrastructure protection with innovative SECurity framework. https://www.cipsec.eu/, 2019 (accessed February 9th 2023).
[43] RESilient transport InfraSTructure to extreme events. https://www.resistproject.eu/, 2018 (accessed February 9th 2023).
[44] Preparedness and resilience enforcement for critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection https://www.precinct.info/en/publications/, 2021 (accessed February 9th 2023).
[45] Wang S, Gu X, Chen J, Chen C, Huang X. Robustness improvement strategy of cyber-physical systems with weak interdependency. Reliab Eng Syst Saf 2023;229:108837.
[46] Tu H, Xia Y, Wu J, Zhou X. Robustness assessment of cyber–physical systems with weak interdependency. Physica A: Stat Mech Appl 2019;522:9–17.
[47] Zhang Y, Yağan O. Robustness of interdependent cyber-physical systems against cascading failures. IEEE Trans Automat Contr 2019;65:711–26.
[48] Derrible S, Kennedy C. Applications of graph theory and network science to transit network design. Transp Rev 2011;31:495–519.
[49] Gordan M, Kountche DA, McCrum D, Schauer S, König S, Delannoy S, Connolly L, Iacob M, Durante NG, Shekhawat Y. Protecting critical infrastructure against cascading effects: the PRECINCT approach. Resilient Cities Struct 2024;3:1–19.
[50] Patel P, Narmawala Z, Thakkar A. A survey on intelligent transportation system using internet of things. In: Emerging Research in Computing, Information, Communication and Applications: ERCICA 2018, 1; 2019. p. 231–40.
[51] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 2019;7:82721–43.
[52] Ntafloukas K, Pasquale L, Martinez-Pastor B, McCrum DP. A vulnerability assessment approach for transportation networks subjected to cyber–physical attacks. Future Internet 2023;15:100.
[53] Stellios I, Kotzanikolaou P, Grigoriadis C. Assessing IoT enabled cyber-physical attack paths against critical systems. Comput Secur 2021;107:102316.
[54] Lai R, Qiu X, Wu J. Robustness of asymmetric cyber-physical power systems against cyber attacks. IEEE Access 2019;7:61342–52.
[55] Xu L, Guo Q, Yang T, Sun H. Robust routing optimization for smart grids considering cyber-physical interdependence. IEEE Trans Smart Grid 2018;10:5620–9.
[56] Zhang P, Cheng B, Zhao Z, Li D, Lu G, Wang Y, Xiao J. The robustness of interdependent transportation networks under targeted attack. Europhys Lett 2013;103:68005.
[57] Kermanshah A, Derrible S. Robustness of road systems to extreme flooding: using elements of GIS, travel demand, and network science. Natural hazards 2017;86:151–64.
[58] Urlainis A, Ornai D, Levy R, Vilnay O, Shohet IM. Loss and damage assessment in critical infrastructures due to extreme events. Saf Sci 2022;147:105587.
[59] Xu L, Guo Q, Sheng Y, Muyeen S, Sun H. On the resilience of modern power systems: a comprehensive review from the cyber-physical perspective. Renew Sustain Energy Rev 2021;152:111642.
[60] Chen Z, Zhang S, Dui H. Importance-based risk evaluation methodology in transportation cyber-physical systems. Front Eng Manage 2025:1–14.
[61] Ti B, Li G, Zhou M, Wang J. Resilience assessment and improvement for cyber-physical power systems under typhoon disasters. IEEE Trans Smart Grid 2021;13:783–94.
[62] Zhu C, Wu J, Liu M, Luan J, Li T, Hu K. Cyber-physical resilience modelling and assessment of urban roadway system interrupted by rainfall. Reliab Eng Syst Saf 2020;204:107095.
[63] Argyriou I, Tsoutsos T. Assessing critical entities: risk management for IoT devices in ports. J Mar Sci Eng 2024;12:1593.
[64] Kenett DY, Gao J, Huang X, Shao S, Vodenska I, Buldyrev SV, Paul G, Stanley HE, Havlin S. Network of interdependent networks: overview of theory and applications. In: Networks of Networks: The Last Frontier of Complexity; 2014. p. 3–36.
[65] Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. Nature 2010;464:1025–8.
[66] Cheng Z, Cao J. Cascade of failures in interdependent networks coupled by different type networks. Physica A: Stat Mech Appl 2015;430:193–200.
[67] Wu J, You W, Wu T, Xia Y. Abnormal phenomenon in robustness of complex networks with heterogeneous node functions. Physica A: Stat Mech Appl 2018;506:451–61.
[68] Gao Y-L, Chen S-M, Nie S, Ma F, Guan J-J. Robustness analysis of interdependent networks under multiple-attacking strategies. Physica A: Stat Mech Appl 2018;496:495–504.
[69] Zhang Y, Arenas A, Yağan O. Cascading failures in interdependent systems under a flow redistribution model. Phys Rev E 2018;97:022307.
[70] Ji X, Wang B, Liu D, Chen G, Tang F, Wei D, Tu L. Improving interdependent networks robustness by adding connectivity links. Physica A: Stat Mech Appl 2016;444:9–19.
[71] Dong S, Wang H, Mostafavi A, Gao J. Robust component: a robustness measure that incorporates access to critical facilities under disruptions. J R Soc Interface 2019;16:20190149.
[72] National Bridge Inventory (NBI). https://www.fhwa.dot.gov/bridge/nbi.cfm, (accessed August 2023).
[73] Phule RR, Choudhury D. Assessing and mapping seismic liquefaction hazard, vulnerability, and risk of the transportation infrastructure of Mumbai city, India. In: Geotechnical earthquake engineering and soil dynamics V: seismic hazard analysis, earthquake ground motions, and regional-scale assessment. Reston, VA: American Society of Civil Engineers; 2018. p. 658–66.
[74] Pitilakis K, Franchin P, Khazai B, Wenzel H. SYNER-G: systemic seismic vulnerability and risk assessment of complex urban, utility, lifeline systems and critical facilities: methodology and applications. Springer; 2014.
[75] Mackie KR, Stojadinović B. Fragility basis for California highway overpass bridge seismic decision making. Pacific Earthquake Engineering Research Center, College of Engineering; 2005.
[76] USGS. https://www.usgs.gov/programs/earthquake-hazards/hazards, (accessed 5th of July 2023).
[77] Danciu L, Nandan S, Reyes CG, Basili R, Weatherill G, Beauval C, Rovida A, Vilanova S, Sesetyan K, Bard P-Y. The 2020 update of the European Seismic Hazard model-ESHM20: model overview. EFEHR Techn Rep 2021;1.
[78] Silva V, Crowley H, Pagani M, Monelli D, Pinho R. Development of the OpenQuake engine, the Global Earthquake Model's open-source software for seismic risk assessment. Nat Hazards 2014;72:1409–27.
[79] Wang Z. Seismic hazard assessment: issues and alternatives. Pure Appl Geophys 2011;168:11–25.
[80] Muntasir Billah A, Alam MShahria. Seismic fragility assessment of highway bridges: a state-of-the-art review. Struct Infrastruct Eng 2015;11:804–32.
[81] Baker JW. Efficient analytical fragility function fitting using dynamic structural analysis. Earthq Spectra 2015;31:579–99.
[82] Costa AC, Sousa M, Carvalho A, Coelho E. Evaluation of seismic risk and mitigation strategies for the existing building stock: application of LNECloss to the metropolitan area of Lisbon. Bull Earthq Eng 2010;8:119–34.
[83] Dong Y, Frangopol DM, Saydam D. Sustainability of highway bridge networks under seismic hazard. J Earthq Eng 2014;18:41–66.
[84] Lee Y-J, Song J, Gardoni P, Lim H-W. Post-hazard flow capacity of bridge transportation network considering structural deterioration of bridges. Struct Infrastruct Eng 2011;7:509–21.
[85] Bocchini P, Frangopol DM. A stochastic computational framework for the joint transportation network fragility analysis and traffic flow distribution under extreme events. Probab Eng Mech 2011;26:182–93.
[86] Huang Z, Wang C, Stojmenovic M, Nayak A. Characterization of cascading failures in interdependent cyber-physical systems. IEEE Trans Comput 2014;64:2158–68.
[87] Muriel-Villegas JE, Alvarez-Uribe KC, Patiño-Rodríguez CE, Villegas JG. Analysis of transportation networks subject to natural hazards–insights from a Colombian case. Reliab Eng Syst Saf 2016;152:151–65.
[88] Zhu F, Lv Y, Chen Y, Wang X, Xiong G, Wang F-Y. Parallel transportation systems: toward IoT-enabled smart urban traffic control and management. IEEE Trans Intell Transport Syst 2019;21:4063–71.
[89] Chong HF, Ng DWK. Development of IoT device for traffic management system. 2016 IEEE Student Conference on Research and Development (SCOReD). IEEE; 2016.
[90] Nogal M, Nápoles OM, O'Connor A. Structured expert judgement to understand the intrinsic vulnerability of traffic networks. Transport Res Part A: Policy Pract 2019;127:136–52.
[91] Kwag S, Ok S-Y. Robust design of seismic isolation system using constrained multi-objective optimization technique. KSCE J Civil Eng 2013;17:1051–63.
[92] Zhou S, Demartino C, Xu J, Xiao Y. Effectiveness of CFRP seismic-retrofit of circular RC bridge piers under vehicular lateral impact loading. Eng Struct 2021;243:112602.
[93] Babar M, Arif F. Real-time data processing scheme using big data analytics in internet of things based smart transportation environment. J Ambient Intell Humaniz Comput 2019;10:4167–77.
[94] Padgett JE, DesRoches R. Retrofitted bridge fragility analysis for typical classes of multispan bridges. Earthq Spectra 2009;25:117–41.
[95] Wright T, DesRoches R, Padgett JE. Bridge seismic retrofitting practices in the central and southeastern United States. J Bridge Eng 2011;16:82–92.
[96] Raychaudhuri S. Introduction to monte Carlo simulation. 2008 Winter simulation conference. IEEE; 2008.
[97] Berglund EZ, Monroe JG, Ahmed I, Noghabaei M, Do J, Pesantez JE, Khaksar Fasaee MA, Bardaka E, Han K, Proestos GT. Smart infrastructure: a vision for the role of the civil engineering profession in smart cities. J Infrastruct Syst 2020;26:03120001.
[98] Pundir A, Singh S, Kumar M, Bafila A, Saxena GJ. Cyber-physical systems enabled transport networks in smart cities: challenges and enabling technologies of the new mobility era. IEEE Access 2022;10:16350–64.
[99] Haroon A, Sagor M, Maurice M, Jin L, Stoleru R, Blalock R. On edge coordination in highly dynamic cyber-physical systems for emergency response. 2022 Workshop on Cyber Physical Systems for Emergency Response (CPS-ER). IEEE; 2022.
[100] Tonelli F, Demartini M, Pacella M, Lala R. Cyber-physical systems (CPS) in supply chain management: from foundations to practical implementation. Procedia CIRP 2021;99:598–603.
[101] Johnson G, Seligson H, Pyun J, Wickens M. Seismic fragility and risk assessment of waterfront structures at the port of San Francisco. 15th Triennial International Conference Reston, VA. American Society of Civil Engineers; 2019.
[102] Lam JC, Adey BT, Heitzler M, Hackl J, Gehl P, Van Erp N, d'Ayala D, van Gelder P, Hurni L. Stress tests for a road network using fragility functions and functional capacity loss functions. Reliab Eng Syst Saf 2018;173:78–93.