SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

System-of-Systems Integration for Civil Infrastructures Resiliency Toward Multi-Hazard Events

Vahid Balali, PhD

CSUTC California State University Transportation Consortium

CALIFORNIA STATE UNIVERSITY LONG BEACH

Mineta Transportation Institute

Founded in 1991, the Mineta Transportation Institute (MTI), an organized research and training unit in partnership with the Lucas College and Graduate School of Business at San José State University (SJSU), increases mobility for all by improving the safety, efficiency, accessibility, and convenience of our nation's transportation system. Through research, education, workforce development, and technology transfer, we help create a connected world. MTI leads the Mineta Consortium for Transportation Mobility (MCTM) funded by the U.S. Department of Transportation and the California State University Transportation Consortium (CSUTC) funded by the State of California through Senate Bill 1. MTI focuses on three primary responsibilities:

Research

MTI conducts multi-disciplinary research focused on surface transportation that contributes to effective decision making. Research areas include: active transportation; planning and policy; security and counterterrorism; sustainable transportation and land use; transit and passenger rail; transportation engineering; transportation finance; transportation technology; and workforce and labor. MTI research publications undergo expert peer review to ensure the quality of the research.

Education and Workforce

To ensure the efficient movement of people and products, we must prepare a new cohort of transportation professionals who are ready to lead a more diverse, inclusive, and equitable transportation industry. To help achieve this, MTI sponsors a suite of workforce development and education opportunities. The Institute supports educational programs offered by the Lucas Graduate School of Business: a Master of Science in Transportation Management, plus graduate certificates that include High-Speed and Intercity Rail Management and Transportation Security Management. These flexible programs offer live online classes so that working transportation professionals can pursue an advanced degree regardless of their location.

Information and Technology Transfer

MTI utilizes a diverse array of dissemination methods and media to ensure research results reach those responsible for managing change. These methods include publication, seminars, workshops, websites, social media, webinars, and other technology transfer mechanisms. Additionally, MTI promotes the availability of completed research to professional organizations and works to integrate the research findings into the graduate education program. MTI's extensive collection of transportation-related publications is integrated into San José State University's world-class Martin Luther King, Jr. Library.

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and accuracy of the information presented herein. This document is disseminated in the interest of information exchange. MTI's research is funded, partially or entirely, by grants from the California Department of Transportation, the California State University Office of the Chancellor, the U.S. Department of Homeland Security, and the U.S. Department of Transportation, who assume no liability for the contents or use thereof. This report does not constitute a standard specification, design standard, or regulation.

Report 23-15

System-of-Systems Integration for Civil Infrastructures Resiliency Toward Multi-Hazard Events

Vahid Balali, PhD

August 2023

A publication of the
Mineta Transportation Institute
Created by Congress in 1991

College of Business
San José State University
San José, CA 95192–0219

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. 23-15	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle System-of-Systems Integration for Civil Infrastructures Resiliency Toward Multi-Hazard Events		**5. Report Date** August 2023
		6. Performing Organization Code
7. Authors Vahid Balali, PhD		**8. Performing Organization Report** CA-MTI-2245
9. Performing Organization Name and Address Mineta Transportation Institute College of Business San José State University San José, CA 95192–0219		**10. Work Unit No.**
		11. Contract or Grant No. ZSB12017-SJAUX
12. Sponsoring Agency Name and Address State of California SB1 2017/2018 Trustees of the California State University Sponsored Programs Administration 401 Golden Shore, 5th Floor, Long Beach, CA 90802		**13. Type of Report and Period Covered**
		14. Sponsoring Agency Code

15. Supplemental Notes

16. Abstract

Civil infrastructure systems—facilities that supply principal services, such as electricity, water, transportation, etc., to a community—are the backbone of modern society. These systems are frequently subject to multi-hazard events, such as earthquakes. The poor resiliency of these infrastructures results in many human casualties and significant economic losses every year. An outline of a holistic view that considers how different civil infrastructure systems operate independently and how they interact and communicate with each other is required to have a resilient infrastructure system. More specifically a systems engineering approach is required to enable infrastructure to remain resilient in the case of extreme events, including natural disasters. To address these challenges, this research builds on the proposal that the infrastructure systems be equipped with state-of-the-art sensor networks that continuously record the condition and performance of the infrastructure. The sensor data from each infrastructure are then transferred to a data analysis system component that employs artificial intelligence techniques to constantly analyze the infrastructure's resiliency and energy efficiency performance. This research models the resilient infrastructure problem as a System of Systems (SoS) comprised of the abovementioned components. It explores system integration and operability challenges and proposes solutions to meet the requirements of the SoS. An integration ontology, as well as a data-centric architecture, is developed to enable infrastructure resiliency toward multi-hazard events. The Federal Emergency Management Agency (FEMA), and infrastructure managers, such as Departments of Transportation (DOTs) and the Federal Highway Administration (FHWA), can learn from and integrate these solutions to make civil infrastructure systems more resilient for all.

17. Key Words Resilience, Resilient Infrastructure System, System Integration, System of Sytems (SoS), Multi-Hazard Events	**18. Distribution Statement** No restrictions. This document is available to the public through The National Technical Information Service, Springfield, VA 22161.		
19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 37	**22. Price**

DOI: 10.31979/mti.2023/2245

Mineta Transportation Institute
College of Business
San José State University
San José, CA 95192–0219

Tel: (408) 924–7560
Fax: (408) 924–7565
Email: mineta-institute@sjsu.edu
transweb.sjsu.edu/research/2245

ACKNOWLEDGMENTS

I would like to thank the National Center for Transportation, Green Technology, and Education (TransGET) at California State University Long Beach. Funding for this research was provided by the State of California SB1 2022/2023 through the Trustees of the California State University (Agreement # ZSB12017-SJAUX) and the California State University Transportation Consortium (CSUTC). This report is based in part on work supported by the CSUTC. Any opinions, findings, conclusions, or recommendations expressed in this report are those of the author and do not necessarily reflect the views of the CSUTC or other sponsors.

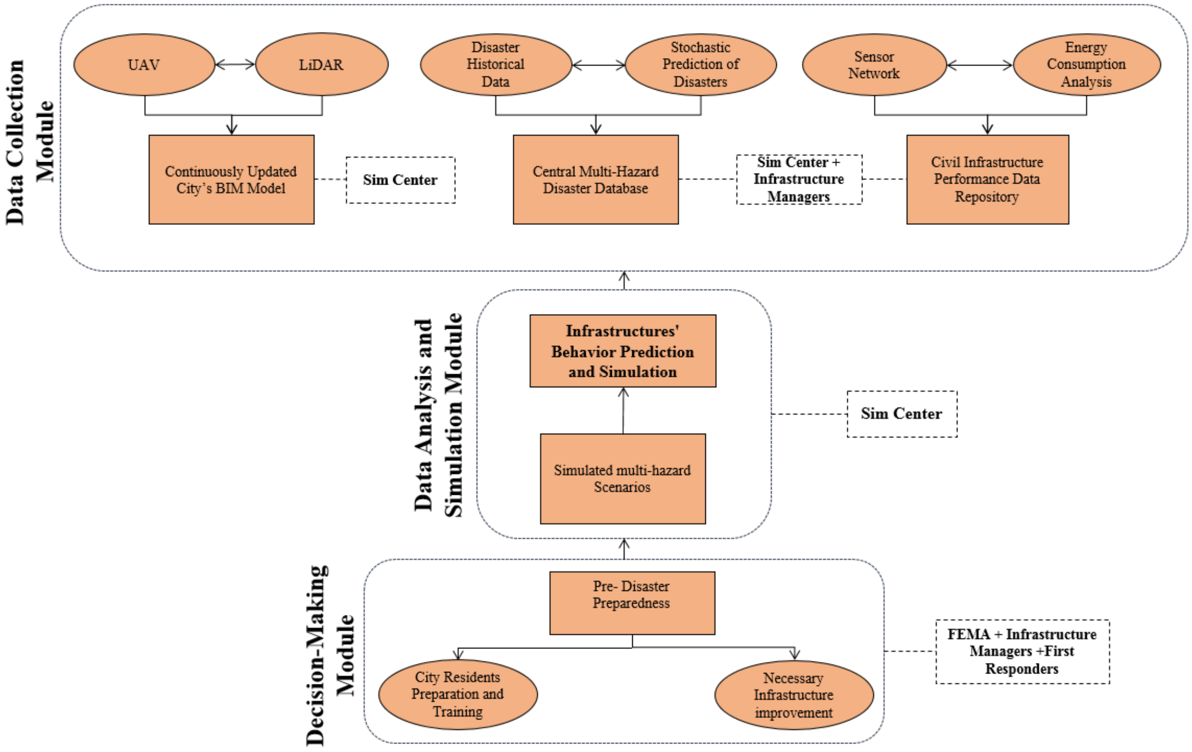
CONTENTS

LIST OF FIGURES

LIST OF TABLES

Executive Summary

Developing a unified System Integration (SI) ontology would reduce the complexity of civil infrastructure, especially for cases in which resiliency and adaptability are required. The main stakeholders of resilient civil infrastructure systems, their requirements, concerns, integration resources, and mechanisms to develop an SI ontology are identified for this project. There are several system components involved in this research. These components, at the infrastructure level, are operated and managed independently and their functionalities do not necessarily depend on each other. However, integrating these components creates a new system that is capable of evaluating the resiliency of all the infrastructures within the city and, consequently, of the city itself. Due to a large number of components, the independence of the involved components in operation and management, and the large geographic extent of the component systems, the system is modeled and studied as a System of Systems (SoS). A complex SoS is undesirable since any compromise in information transfer and access would jeopardize the objective of the system and would potentially put citizens in danger. The research team adopts a Directed type of SoS since the system's objective is to provide resiliency for the infrastructures of a city and, therefore, the system must be centrally managed to align individual infrastructures' resiliency levels with the city's resiliency requirements. The system components (infrastructures within the city) operate independently to maintain their resiliency. However, their behavior is subordinated to the city's resiliency. Although the SoS is comprised of multiple systems and databases, a Directed SoS is preferred over an Acknowledged SoS since the purposes of all the systems deal exclusively in resiliency. The overall architecture of the proposed SoS is shown here.

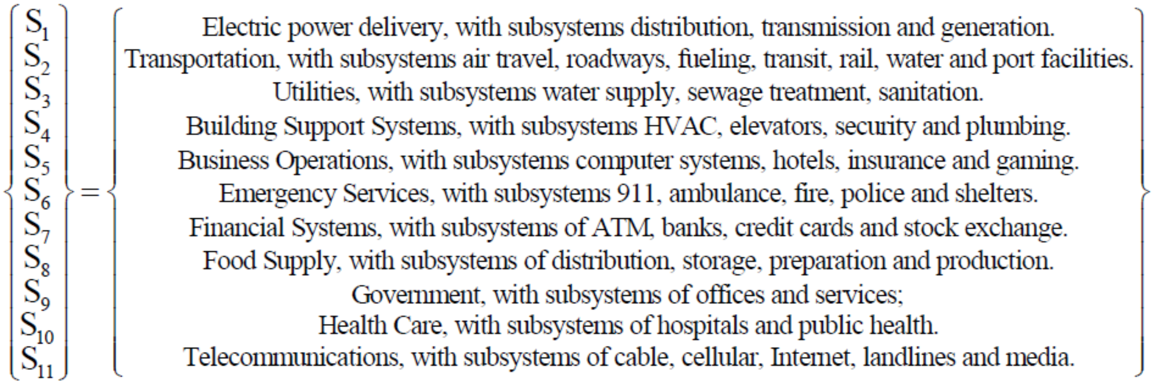

Data Collection Module
UAV
LiDAR
Disaster Historical Data
Stochastic Prediction of Disasters
Sensor Network
Energy Consumption Analysis
Continuously Updated City's BIM Model
Sim Center
Central Multi-Hazard Disaster Database
Sim Center + Infrastructure Managers
Civil Infrastructure Performance Data Repository
Data Analysis and Simulation Module
Infrastructures' Behavior Prediction and Simulation
Simulated multi-hazard Scenarios
Sim Center
Decision-Making Module
Pre- Disaster Preparedness
City Residents Preparation and Training
Necessary Infrastructure improvement
FEMA + Infrastructure Managers +First Responders

1. Introduction and Background

Civil infrastructure systems are the backbone of the modern economy and the quality of life of society since they are the principal service suppliers and the main energy consumers. These systems are usually interrelated and therefore they are often represented as nodes within a region's infrastructure network. A minor defect in one of the nodes could directly or indirectly affect the operation of the other nodes. Occasionally, due to the multifaceted interconnections of these infrastructure systems, failure in one system could result in a cascading effect that is destructive for the network and makes the recovery of some systems highly challenging. For instance, an electric power outage could impact the services of other infrastructures such as water supplies and transportation services [1].

Civil infrastructure systems expand rapidly due to increases in the needs of society and grow into more complex systems. These systems are comprised of a complex network of interdependent subsystems that are closely connected with multi-purpose objectives [2]. Reed, Zabinsky, and Boyle [2] represented the eleven-system interdependent infrastructure network model developed by Chang, McDaniels, and Reed [3] as indicated in Figure 1:

Figure 1. Eleven-System Interdependent Model



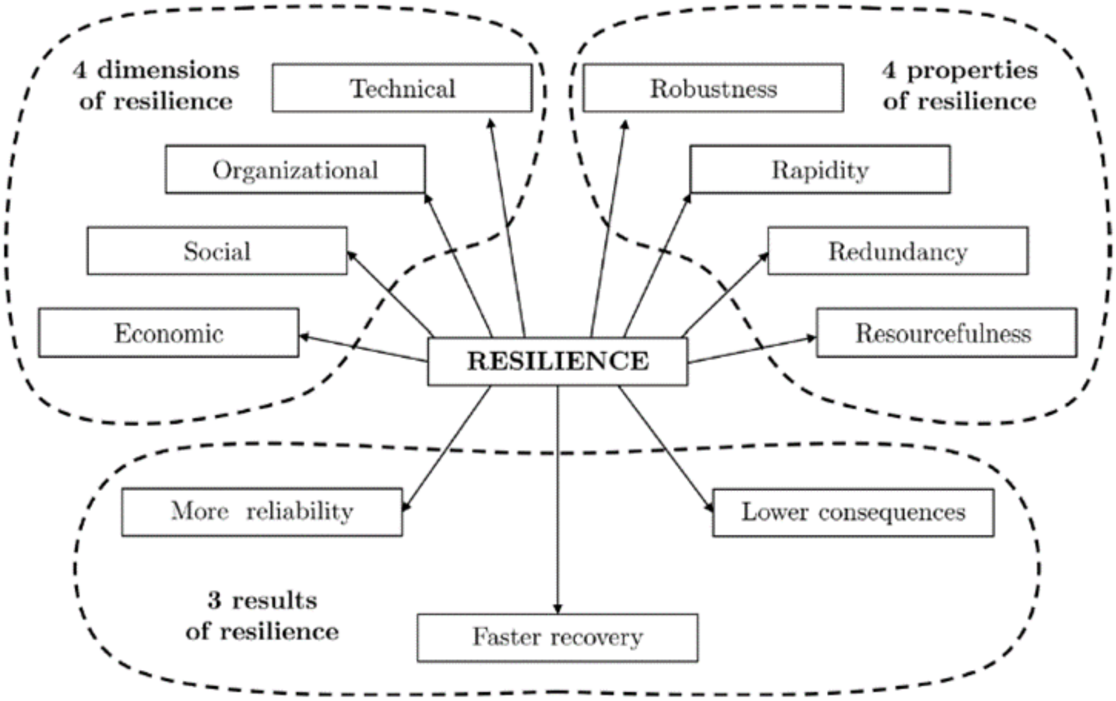
$$\begin{Bmatrix} S_1\\ S_2\\ S_3\\ S_4\\ S_5\\ S_6\\ S_7\\ S_8\\ S_9\\ S_{10}\\ S_{11} \end{Bmatrix} = \begin{Bmatrix} \text{Electric power delivery, with subsystems distribution, transmission and generation.}\\ \text{Transportation, with subsystems air travel, roadways, fueling, transit, rail, water and port facilities.}\\ \text{Utilities, with subsystems water supply, sewage treatment, sanitation.}\\ \text{Building Support Systems, with subsystems HVAC, elevators, security and plumbing.}\\ \text{Business Operations, with subsystems computer systems, hotels, insurance and gaming.}\\ \text{Emergency Services, with subsystems 911, ambulance, fire, police and shelters.}\\ \text{Financial Systems, with subsystems of ATM, banks, credit cards and stock exchange.}\\ \text{Food Supply, with subsystems of distribution, storage, preparation and production.}\\ \text{Government, with subsystems of offices and services;}\\ \text{Health Care, with subsystems of hospitals and public health.}\\ \text{Telecommunications, with subsystems of cable, cellular, Internet, landlines and media.} \end{Bmatrix}$$

(Figure directly adopted from Reed, Zabinsky, and Boyle 2011).

SI is an important concern with systems similar to civil infrastructure systems, especially in cases in which resiliency and adaptability are required [4]. The resiliency and sustainability of civil infrastructure systems have been widely studied in the last few years. Bruneau et al. [5] defined the dimensions, properties, and results of resiliency, as represented in Figure 2. The two terms—sustainability and resiliency—are often used interchangeably, but there are a few fundamental differences between them. In general, sustainability concerns how the environment is affected by the operation of infrastructures while resiliency is concerned with the reaction of the infrastructure network and human communities to extreme events. Additionally, resiliency concentrates on the pace of recovery once a hazardous event takes place while sustainability focuses on how to efficiently consume natural resources considering the needs of future generations.

Bocchini et al. [6] provided a detailed and comprehensive study comparing the two concepts. They argued that the two concepts are complementary and should be used in an integrated approach. They also provided a table of similarities and differences between sustainability and resiliency for different categories, including measuring labels, quantification methods, spatial scales, and targets. They studied the sustainability and resiliency performance of two types of bridges (a girder bridge and a frame bridge) during their simulated lifecycle. The sustainability analysis was done for two impact categories of global warming and total primary energy while the resiliency of the bridges was studied in the scenario of an earthquake with a 2,475-year return period. Their sustainability and resiliency studies for the bridges were different from other similar works because they used a probabilistic analysis and allocated distinct probabilities of occurrence and risks for damages with different levels of severity. One of their key conclusions was that the collection of performance data from civil infrastructures for sustainability and resiliency studies is still a gap in the literature.

Figure 2. Different Aspects of Resiliency According to Bruneau Et Al. 2003



(Diagram directly adopted from Bocchini et al. 2014).

Ouyang and Duenas-Osorio [7] proposed a three-stage framework for the evaluation of the resiliency of a smart grid based on the fact that the resiliency of infrastructure is comprised of three main stages: resistance, absorbance, and recovery. The resiliency outcomes for different improvement strategies were represented using a restoration curve. The results indicated that in cases of a limited number of recovery resources, employing better recovery sequences would result in maximum resiliency. Additionally, their study showed that by using improvement strategies in all three stages, the annual resiliency of the smart grid was increased by less than 0.5 percent in comparison with the original grid.

Mostafavi et al. [8] also pointed out that civil infrastructure is essentially built from various independent and interdependent systems and stakeholders and, therefore, an SoS approach would be suitable to study their behavior. Mostafavi and Abraham [9] proposed a framework comprised of a bottom-up approach for resiliency-based infrastructure planning that focused on prioritizing infrastructure systems renewal for resource allocation. Reed, Zabinsky, and Boyle [2] proposed a framework for increasing resiliency, particularly for post-disaster decision-making. The framework was built on a Multi-Objective Interacting Particle (MOIP) algorithm which was based on If-Then rule-based reasoning. They compared their framework's performance with a traditional method for post-disaster recovery from a case-study earthquake. Their study indicated that the proposed MOIP solution provides more rapid recovery and timely resource allocation for bringing transportation infrastructure back online. While such work has focused on the financial aspects of the recovery stage in the resiliency of civil infrastructures, there is other work that has studied the absorbance stage of resiliency.

Brownjohn and Aktan [10] discussed the need for condition assessment and the monitoring of the structural performance of bridge facilities to ensure their resiliency, especially the need for integrating state-of-the-art structural health monitoring methods with decision-making processes. Their study points out that structural health monitoring technology is maturing. However, a systematic approach is needed to fuse the data from the monitoring process with methodical decision-making.

The focus of all the above studies is mainly on how to be resilient considering the current condition of civil infrastructures. However, there is a gap in the literature concerning the definition of a holistic view using systems engineering principles to improve the resiliency of the infrastructures by enhancing their acceptance. To increase the absorbance capability of the infrastructures, it is required to collect a comprehensive set of performance data from the infrastructure to identify its deficiencies in terms of resiliency. The contribution to the problem of integration for civil infrastructure resiliency toward multi-hazard events in this paper is two-fold: (1) develop a digital semantic data repository of all the civil infrastructure systems within a specified geographical region; and (2) provide a simulation that analyzes, and computing technologies that analyze, the input data from different infrastructures and proactively evaluate their resiliency against probable, multi-hazard, and extreme events.

2. System's Definition and Typology

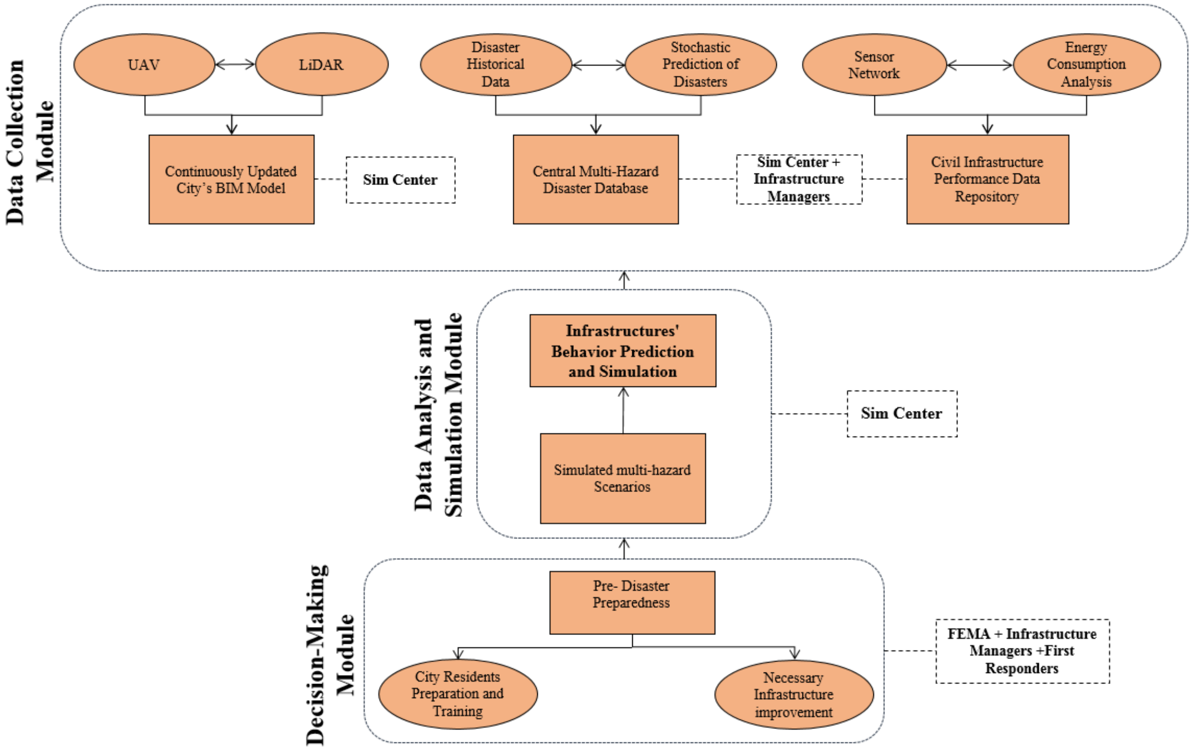
Civil infrastructure systems generally consist of an array of facilities that supply principal services, such as electricity, water, transportation, and more, to a community. The size of the community under investigation defines the system boundary. The system boundary could range from a city to broader geographical scopes, such as a county, state, or country. This paper focuses on the resiliency of civil infrastructures at the city level; however, by representing every city in the nation as a node of a broader network, the results of this study could be extended to the national level.

This study builds on the hypothesis that the engagement of civil infrastructures within a city, along with the communities who live in that city, could be improved by continuously collecting data on the performance and resiliency conditions of the civil infrastructures and the city in general. The ultimate vision of this study is to have a digital semantic representation of a city and all its supplying infrastructures. In order to realize this vision, infrastructures must be equipped with smart sensors that constantly report their condition, so that information on the resiliency of infrastructures can be derived continuously. Each infrastructure must have a database as well as a main server to store all the data received from the sensors. A computing component must be implemented in each infrastructure to connect to the server and retrieve performance data, analyze it, and evaluate resiliency as well as the sustainability status of the infrastructure. All the infrastructures' databases must be connected to a central data warehouse that stores and consolidates all the information and analyzes the resiliency and sustainability of the infrastructures at a city level. The digital information of all the buildings including residential or commercial building types provided by the civil infrastructures even though the consumers of the services are within the city.

Three-dimensional digital models of the infrastructures and the buildings are created using Building Information Modeling (BIM) technology and are regularly updated using state-of-the-art remote sensing imaging tools such as 3D laser scanners and unmanned aerial vehicles (UAV). This information enables the evaluation of the resiliency of the infrastructures with respect to the users of their services. In addition, this information facilitates the prediction of the city's behavior in various probable extreme events using 3D simulations. The last component of the proposed system is the installation of black boxes in secure places in each infrastructure. The key mission of these black boxes is to acquire and store data when extreme events occur and other acquisition systems are dysfunctional. The black boxes store the latest condition of the infrastructure, and their data can be used to estimate the damages incurred by the infrastructure after extreme events.

There are several system components involved in this study. These components, at the infrastructure level, are operated and managed independently, and their functionalities do not necessarily depend on each other. However, integrating these components creates a new system that is capable of evaluating the resiliency of all the infrastructures within the city and, consequently, of the city itself. Due to a large number of components, the independence of the involved components in operation and management, and the large geographic extent of the component systems, the system is modeled and studied as an SoS. A complex SoS is undesirable since any compromise in information transfer and access would jeopardize the objective of the system, and would potentially put citizens in danger. The author adopts a Directed type of SoS because the system's objective is to provide resiliency for the infrastructures of a city and, therefore, the system must be centrally managed to align individual infrastructures' resiliency levels with the city's resiliency requirements. The system components (infrastructures within the city) operate independently to maintain their resiliency. However, their behavior is subordinate to the city's resiliency [11]. Although the SoS is comprised of multiple systems and databases, a Directed SoS is preferred over an Acknowledged SoS since the purposes of all the systems deal exclusively in resiliency. Figure 3 illustrates the overall architecture of the proposed SoS. Sim Center, FEMA, and infrastructure managers are the main stakeholders of the SoS.

Figure 3. Resilient Civil Infrastructures System Architecture


Data Collection Module
UAV
LiDAR
Disaster Historical Data
Stochastic Prediction of Disasters
Sensor Network
Energy Consumption Analysis
Continuously Updated City's BIM Model
Sim Center
Central Multi-Hazard Disaster Database
Sim Center + Infrastructure Managers
Civil Infrastructure Performance Data Repository
Data Analysis and Simulation Module
Infrastructures' Behavior Prediction and Simulation
Simulated multi-hazard Scenarios
Sim Center
Decision-Making Module
Pre- Disaster Preparedness
City Residents Preparation and Training
Necessary Infrastructure improvement
FEMA + Infrastructure Managers +First Responders

3. System of Systems Integration Ontology

This section outlines the Systems Integration (SI) semantics by defining the factors that affect the management of SI using a unified SI ontology similar to the one described by Madni and Sievers [4]. Developing a unified SI ontology would reduce the complexity of civil infrastructure, especially when studying an SoS. The main stakeholders of resilient civil infrastructure systems, their requirements, concerns, integration resources, and mechanisms to develop an SI ontology are identified for this study.

3.1 Definition of Stakeholders and their Requirements

There are three main stakeholders identified for this study. The first stakeholder is the U.S. Federal Emergency Management Agency (FEMA). FEMA is in charge of protecting citizens' safety in cases of hazardous events. The agency is responsible for preparing citizens for natural hazards and for training them to recover faster after hazardous events take place. It is essential that FEMA be informed of the present condition of civil infrastructures in order to provide effective remedial plans in the event of extreme events of varying severity. Specifically, FEMA is obligated to coordinate with first responder units based on the criticality of needs, available resources, and aftermath conditions to expedite the recovery process for citizens. Therefore, FEMA communicates directly with infrastructure managers (IMs), who are the second stakeholder of the defined SoS.

IMs are concerned with the resiliency and sustainability status of the infrastructure under their management. Their objective is to improve the condition of the infrastructure according to a cost-effective process. Additionally, they attend to the absorbance capabilities of the infrastructure, as well as response and recovery time after extreme events. They are required to provide information and documents regarding the most up-to-date condition of the infrastructure they manage to FEMA monthly. To get informed about the resiliency and sustainability condition of their infrastructure, they hire the third stakeholder of the defined system—the Sim Center.

The Sim Center is introduced to the system by the association of IMs. All of its processes are managed directly by IMs under their specific governance and according to FEMA's standards. To achieve IMs' requirements, the Sim Center installs smart sensor networks throughout their infrastructures to collect performance data for resiliency and sustainability analysis. The Sim Center coordinates with IMs to identify the best locations for the installation of the sensors and, with the support of the managers, they establish designated computing components, databases, and servers to retrieve data and perform local analysis. In addition, they are required to install black boxes in secure areas within the infrastructures. It is also the Sim Center's responsibility to perform regular maintenance of the sensors and all their cyber systems. Moreover, the Sim Center is required to establish a central data warehouse along with a computing component and a central server to collect data from all the civil infrastructures of the city. These data are then used to perform collective resiliency and sustainability studies at the city level. They are also required to integrate the most up-to-date BIM models of all the buildings throughout the city into the analysis. The Sim Center acquires updated geometrical information from the city and infrastructures using remote sensing technologies, such as LiDAR (Light Detection and Ranging) devices, 3D laser scanners, and UAV systems, while cooperating with IMs and third parties. The Sim Center performs repeated resiliency analyses using the collected data as well as stochastic-based simulations to predict the civil infrastructures' and the city's resiliency towards multi-hazard extreme events. Finally, the Sim Center identifies and reports structural improvements that are necessary for each infrastructure to resist extreme events, at which stage the IMs are required to take corrective actions to improve the condition of the infrastructure. Table 1 summarizes the SoS's stakeholders, their concerns, influences, and metrics.

Table 1. Resilient Infrastructures Stakeholders.

Stakeholder	Concerns	Influences	Metrics
FEMA	- Safety of citizens - Plans, preparation, and mitigation of the effects of the extreme events - Effective remedial plans in case of extreme events - Response and recovery of critical infrastructures that provide vital service to citizens	- Governance - Coordination with first responders - Coordination with infrastructure managers - Preparedness of communities	- Severity of damages and number of casualties - Response level and recovery time of critical infrastructures
Sim Center	- Achievement of infrastructure managers' requirements - Sensor network system's integrity - Responsiveness and promptness of the computing component - Interoperability of the infrastructures - Sensors' regular maintenance	-Risk assessment & management - Stochastic analysis method - Artificial intelligence and data mining methods - Sensor network connections and operations	- Data transfer speed - Computing accuracy and precision - Simulation accuracy
Infrastructure Manager (Private or Public sector)	- Infrastructure's sustainability and resiliency - Cost associated with the required improvements for the resiliency of the infrastructure - Response, absorbance, and the recovery time of the infrastructure in case of extreme events	- Governance - Management of the infrastructure - Coordination with other infrastructure managers - Coordination with FEMA	- Resiliency and sustainability score of the infrastructure - Incurred cost

3.2 Governance

Governance considerations generally consist of FEMA's standard resiliency requirements as well as codes, protocols, and design requirements defined by federal agencies, such as the U.S. DOT (Department of Transportation), FHWA (Federal Highway Administration), etc., who act as IMs in the defined SoS. As far as sustainability is concerned, the U.S. Environmental Protection Agency's rules and regulations must be considered in the SoS integration. National cybersecurity requirements must also be satisfied since the data that drives the whole system is extremely sensitive, given that it includes detailed information about the performance and operation of critical infrastructures. The U.S. General Services Administration's codes and requirements for building information modeling govern the 3D modeling of the city's buildings and infrastructures. Lastly, the Federal Aviation Administration's regulations, in particular, its flying elevation constraints, must be followed in case of the use of drones for condition documentation of the city.

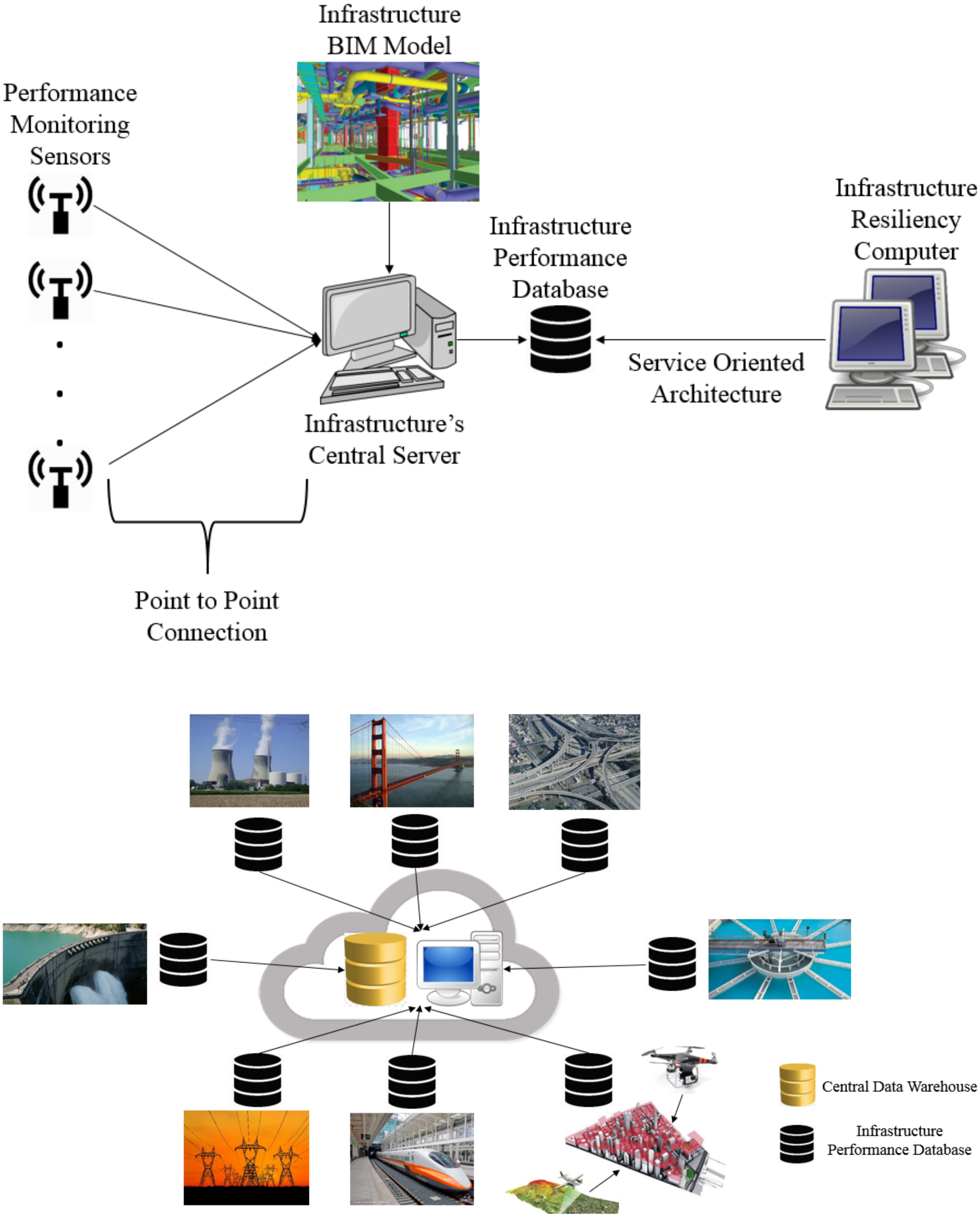
3.3 Structure

The SoS integration requires that the sub-elements of the system be able to communicate effectively through designed interfaces [4]. There are two sets of sub-elements within the SoS that must communicate continuously with each other. The lower-level sub-elements are the smart sensors within each infrastructure that are all connected to their infrastructure's main server while their data is stored in their infrastructure's centralized database (top of Figure 4). At the higher level, the entire infrastructure of the city shares its updated data with the centralized data warehouse located at the Sim Center (bottom of Figure 4).

At the infrastructure level, the sensor networks have a point-to-point connection with the infrastructure's central server through a star network. A star network is adopted rather than a mesh network in order to reduce the complexity of the system. Star networks are simpler than mesh networks, since the latter require complex software and also have more predictable power requirements. Two types of connection may be used for the communication systems in the infrastructure. The default connection between the sensors and the server is established through a wireless network. However, if there exist functional constraints and limitations, then a wired connection is used. Every sensor sends its retrieved data to the server, and the server identifies the corresponding sensor, controls the integrity of the received data, and stores it in the appropriate table within the database. The server provides a web interface to represent the data from the sensors. This interface is used by human operators to manage the network and inspect the data flow. The server also stores the updated BIM model of the infrastructure and integrates the information from the BIM model with the related sensor data before storing them in the database. A computing component is devised for each infrastructure to fetch data from the centralized database to perform resiliency and sustainability analysis. The component is connected to the database through a Service Oriented Architecture (SOA).

At the city level, all the infrastructure databases are connected to a centralized data warehouse in a Service Model-SaaS-based cloud system. The cloud is managed purely by the Sim Center and, therefore, infrastructure managers do not have any control over the cloud infrastructure. The data warehouse integrates the data from all infrastructures with the city's updated BIM model, organizes the data, and prepares them for the required aggregated city-level resiliency analysis. The city's updated BIM model is received through a middleware that converts the models acquired by remote sensing imaging devices to a standard BIM format. A GPU-based computing component connects to the data warehouse using an SOA and executes resiliency and sustainability analysis. The data warehouse structure allows the computing component to perform pattern recognition using historical data.

Figure 4. System Integration Structure
Top: Infrastructure-level structure. Bottom: City-level structure.


Infrastructure BIM Model
Performance Monitoring Sensors
Infrastructure Performance Database
Infrastructure Resiliency Computer
Service Oriented Architecture
Infrastructure's Central Server
Point to Point Connection
Central Data Warehouse
Infrastructure Performance Database

The computing components at the infrastructure level and city level operate primarily according to artificial intelligence and data mining techniques. To carry out complicated resiliency analysis, the computing components must run complex nested queries on the data stored in the databases and the centralized data warehouse. To facilitate the query operation, an Online Analytical Processing (OLAP) approach is adopted for this project. The OLAP approach is widely used to handle multi-dimensional analytical queries on big data for data mining purposes. To implement the OLAP system, the relational databases in the infrastructures and the data warehouse are structured based on a star schema in order to create the OLAP cube as the backbone of the OLAP system. The computing component fetches records from the fact table and derives dimensions from dimension tables. Figure 5 represents a sample star schema designed to derive performance data of different structural components of a bridge. The fact table records measures of a infrastructure structural elements, such as piers, girders, deck, abutment, and foundation, along with the time at which the data is recorded by the embedded sensors. A sample query, presented in Figure 6, aims to identify structural elements that have experienced excessive settlement. Consequently, the elements with excessive settlements are categorized as critical and will be reported to the infrastructure manager.

Figure 5. Star Schema Proposed for Storing Performance Data of a Bridge

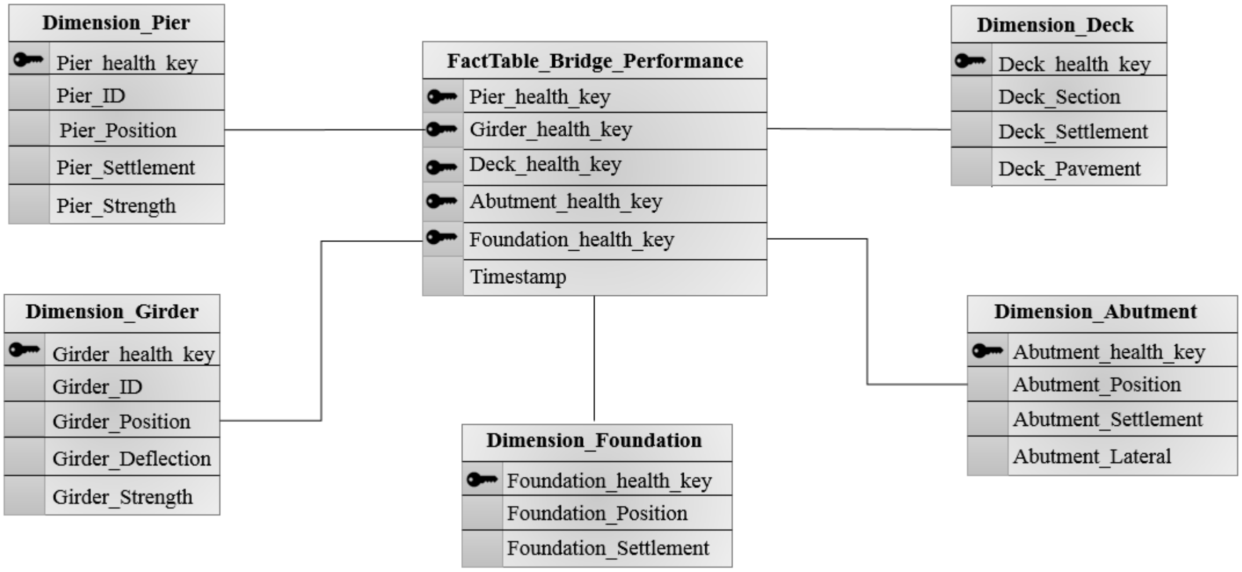
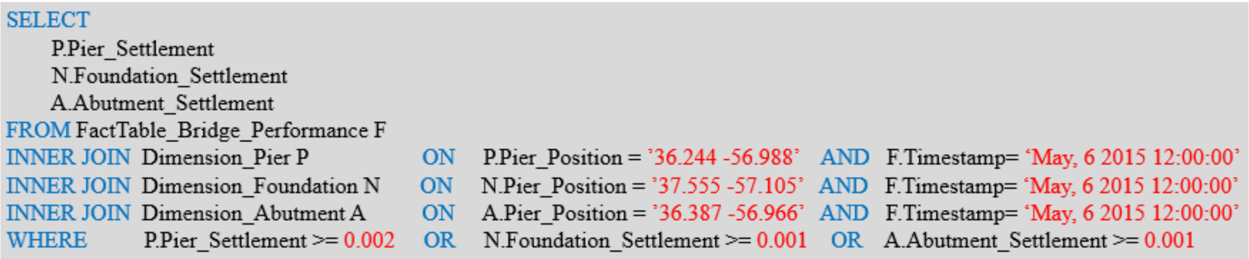


Figure 6. Sample Query for Identifying Structural Elements with Excessive Settlement



```
SELECT
      P.Pier_Settlement
      N.Foundation_Settlement
      A.Abutment_Settlement
FROM FactTable_Bridge_Performance F
INNER JOIN  Dimension_Pier P           ON    P.Pier_Position = ’36.244 -56.988’    AND   F.Timestamp= ‘May, 6 2015 12:00:00’
INNER JOIN  Dimension_Foundation N     ON    N.Pier_Position = ’37.555 -57.105’    AND   F.Timestamp= ‘May, 6 2015 12:00:00’
INNER JOIN  Dimension_Abutment A       ON    A.Pier_Position = ’36.387 -56.966’    AND   F.Timestamp= ‘May, 6 2015 12:00:00’
WHERE          P.Pier_Settlement >= 0.002    OR    N.Foundation_Settlement >= 0.001    OR    A.Abutment_Settlement >= 0.001
```

3.4 Integration Resources and Mechanisms

As discussed in the previous section, unified metadata and the OLAP approach are used to create relational databases and a data warehouse for storing performance data. Sequential Query Language is used to run queries on the databases. Ubiquitous computing methods are integrated with artificial intelligence and data mining methods to continually analyze the resiliency of infrastructures. Remote sensing devices such as different types of LiDAR systems and UAVs are used to document the updated geometric status of the infrastructures and buildings in the city. These devices are also used post-disaster to keep a record of the damages and changes made to the city. Various types of sensors are used to record the structural health conditions of the infrastructures. Wireless networks as well as wired connections are used to transfer data from sensors to servers.

As discussed earlier, the critical structural elements within infrastructure and building systems (e.g., HVAC and mechanical) are equipped with smart sensors. The sensors are connected to the infrastructure's server via wireless and wired connections. The server is connected to the infrastructure's database to store all the data from the sensors in specific tables. The infrastructure's computing component is connected to the database to fetch data and the database is connected to the Sim Center's central data warehouse, which is governed by a cloud system.

3.5 External Influences and Risk Management

Several risk elements must be considered during system integration. Factors such as weather conditions must be considered when installing the smart sensors. The sensors must either be located in parts of the infrastructure that are not exposed to severe weather or they must be protected by special containers. Note that the sensors are not designed to remain functional during extreme events. The black boxes are designed for such circumstances. Black boxes store data only for a limited period and their memory is formatted frequently. They are designed to exclusively collect critical performance data during extreme events. Another external influence that could lead to the destruction of sensors is vandalism. Therefore, the sensors installed in infrastructures that have open access to the public must be concealed in locations that are relatively inaccessible. Energy supply is always a concern as the system's operation is heavily dependent on it. Back-up generators must be installed to support the connections during a power outage. In addition, the wireless networks must be supported by backup modems and routers. Finally, penetration of hackers and malware into the system must be prevented with a proper cyber-security plan (discussed in detail in Section 7).

There is always a risk of losing connection with the database. To avoid this, the database must be connected to the server via a unique IP address and through a secure local connection that is independent from other networks of the infrastructure. Additionally, a secure connection must be established between the centralized data warehouse at the Sim Center and the servers in the infrastructures to ensure fast and reliable data transfer. Lastly, to minimize the risk of inaccurate data analysis and simulations, the computing components in the infrastructures and Sim Center must be continuously monitored by specialists to ensure the integrity and validity of computations.

Since the main feed of the system is the performance data collected from infrastructures, the integrity of the data must be verified frequently. The sensors must also be maintained and calibrated regularly. Uncalibrated sensors produce noisy data that result in erroneous computations. A monitoring component must be designed according to pattern recognition methods to detect noisy or missing data and identify the corresponding uncalibrated sensor. The component shall then raise a red flag and notify the infrastructure manager to fix the sensor.

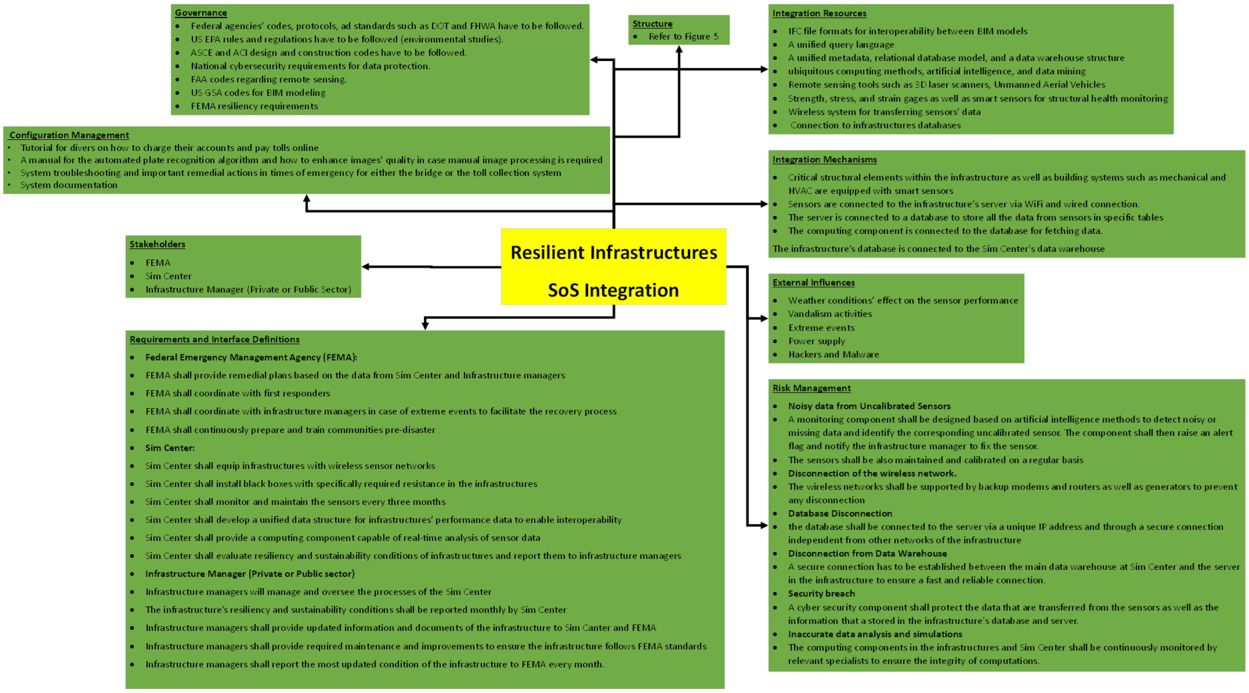
3.6 Configuration Management

Manuals and documents are submitted to the infrastructure managers with information about the implemented sensor network and the locations of the sensors in the infrastructure. Instructions and required information regarding the maintenance of sensors are developed.

3.7 Tailoring and Reuse

As discussed in previous sections, this study focuses on the integration of resilient civil infrastructures at the city level. However, the ultimate goal is to extend this study to larger areas and apply it nationwide. Consequently, the proposed SoS must be designed so that it is replicable at a larger level. The SI must be implemented with the aim of potentially being used all over the country. The system must have enough flexibility for expansion. The key factor in making the system reusable and flexible is interoperability and communication between different components while following a unified standard. Moreover, the SI must be adaptive, meaning that the system components must be designed with plug-and-play integration capabilities. At the city level, when a new infrastructure is added to the system, the central server shall be able to easily recognize it, add it to the network, and consider its input in computations. As a result, the whole system configuration will be applied to entire cities all over the nation. The computing components will be used for similar applications where condition assessment-related tasks are needed. The entire system, including databases, interfaces, and computing components, is updated every six months to adapt to new requirements and advanced technology.

Figure 7. Resilient Civil Infrastructures Sos Integration Ontology



Resilient Infrastructures SoS Integration

Governance

- Federal agencies' codes, protocols, ad standards such as DOT and FHWA have to be followed.
- US EPA rules and regulations have to be followed (environmental studies).
- ASCE and ACI design and construction codes have to be followed.
- National cybersecurity requirements for data protection.
- FAA codes regarding remote sensing.
- US GSA codes for BIM modeling
- FEMA resiliency requirements

Structure

- Refer to Figure 5

Configuration Management

- Tutorial for divers on how to charge their accounts and pay tolls online
- A manual for the automated plate recognition algorithm and how to enhance images' quality in case manual image processing is required
- System troubleshooting and important remedial actions in times of emergency for either the bridge or the toll collection system
- System documentation

Stakeholders

- FEMA
- Sim Center
- Infrastructure Manager (Private or Public Sector)

Requirements and Interface Definitions

- **Federal Emergency Management Agency (FEMA):**
- FEMA shall provide remedial plans based on the data from Sim Center and Infrastructure managers
- FEMA shall coordinate with first responders
- FEMA shall coordinate with infrastructure managers in case of extreme events to facilitate the recovery process
- FEMA shall continuously prepare and train communities pre-disaster
- **Sim Center:**
- Sim Center shall equip infrastructures with wireless sensor networks
- Sim Center shall install black boxes with specifically required resistance in the infrastructures
- Sim Center shall monitor and maintain the sensors every three months
- Sim Center shall develop a unified data structure for infrastructures' performance data to enable interoperability
- Sim Center shall provide a computing component capable of real-time analysis of sensor data
- Sim Center shall evaluate resiliency and sustainability conditions of infrastructures and report them to infrastructure managers
- **Infrastructure Manager (Private or Public sector)**
- Infrastructure managers will manage and oversee the processes of the Sim Center
- The infrastructure's resiliency and sustainability conditions shall be reported monthly by Sim Center
- Infrastructure managers shall provide updated information and documents of the infrastructure to Sim Canter and FEMA
- Infrastructure managers shall provide required maintenance and improvements to ensure the infrastructure follows FEMA standards
- Infrastructure managers shall report the most updated condition of the infrastructure to FEMA every month.

Integration Resources

- IFC file formats for interoperability between BIM models
- A unified query language
- A unified metadata, relational database model, and a data warehouse structure
- ubiquitous computing methods, artificial intelligence, and data mining
- Remote sensing tools such as 3D laser scanners, Unmanned Aerial Vehicles
- Strength, stress, and strain gages as well as smart sensors for structural health monitoring
- Wireless system for transferring sensors' data
- Connection to infrastructures databases

Integration Mechanisms

- Critical structural elements within the infrastructure as well as building systems such as mechanical and HVAC are equipped with smart sensors
- Sensors are connected to the infrastructure's server via WiFi and wired connection.
- The server is connected to a database to store all the data from sensors in specific tables
- The computing component is connected to the database for fetching data.

The infrastructure's database is connected to the Sim Center's data warehouse

External Influences

- Weather conditions' effect on the sensor performance
- Vandalism activities
- Extreme events
- Power supply
- Hackers and Malware

Risk Management

- **Noisy data from Uncalibrated Sensors**
- A monitoring component shall be designed based on artificial intelligence methods to detect noisy or missing data and identify the corresponding uncalibrated sensor. The component shall then raise an alert flag and notify the infrastructure manager to fix the sensor.
- The sensors shall be also maintained and calibrated on a regular basis
- **Disconnection of the wireless network.**
- The wireless networks shall be supported by backup modems and routers as well as generators to prevent any disconnection
- **Database Disconnection**
- the database shall be connected to the server via a unique IP address and through a secure connection independent from other networks of the infrastructure
- **Disconnection from Data Warehouse**
- A secure connection has to be established between the main data warehouse at Sim Center and the server in the infrastructure to ensure a fast and reliable connection.
- **Security breach**
- A cyber security component shall protect the data that are transferred from the sensors as well as the information that a stored in the infrastructure's database and server.
- **Inaccurate data analysis and simulations**
- The computing components in the infrastructures and Sim Center shall be continuously monitored by relevant specialists to ensure the integrity of computations.

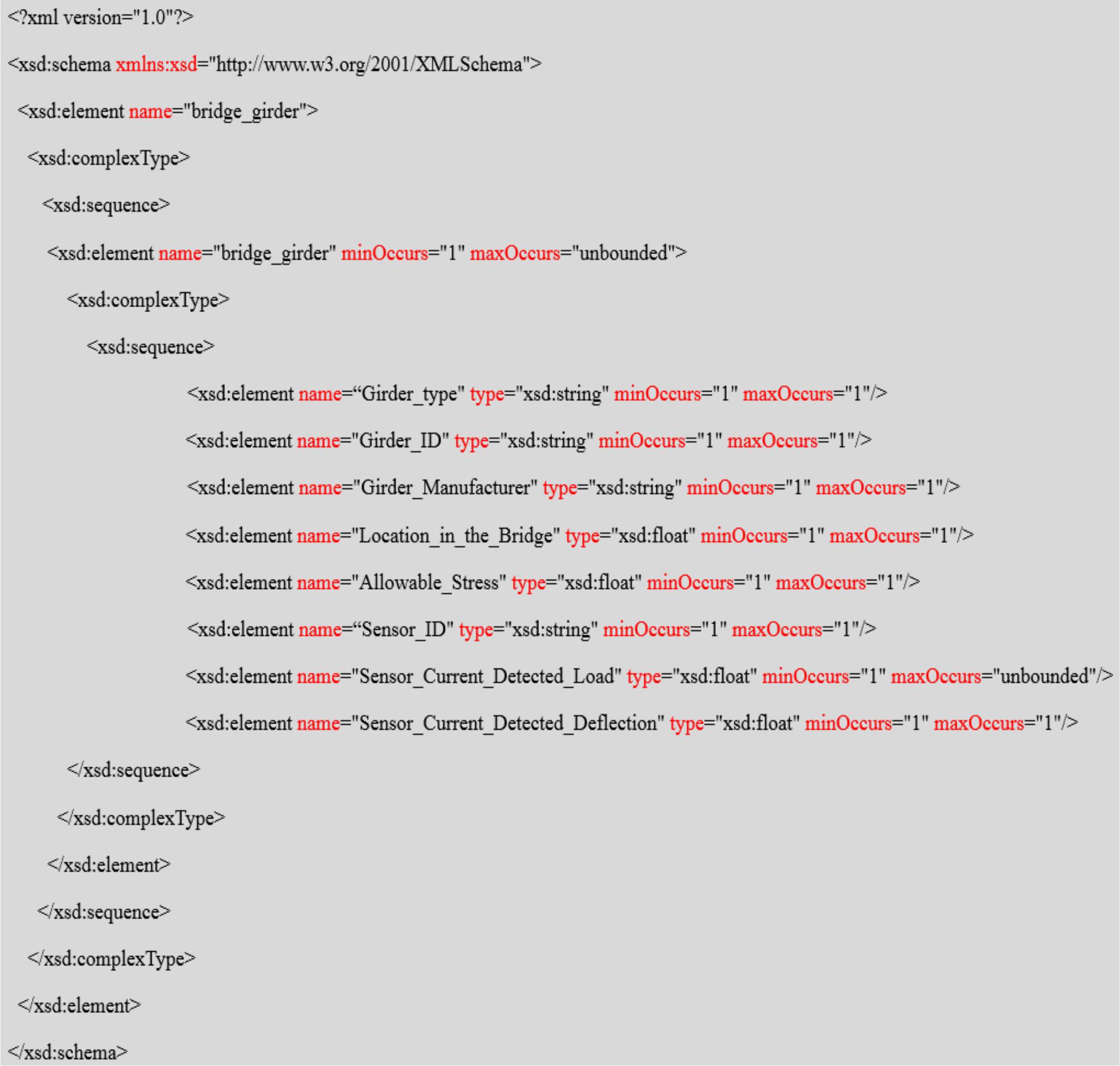
4. Interoperability

The proposed SoS operates based on communication between different civil infrastructures and the server at the Sim Center. Interoperability will be designed into the system from the early integration and implementation stages to make integration easier, more effective, and cheaper. As discussed in the previous section, at the infrastructure level, the server is connected to the infrastructure's database through an SOA, which promotes interoperability. Since the SoS is envisioned for nationwide expansion, another significant motivation for making the SoS interoperable is reusability. There is a need for operational interoperability that enables a common understanding of data that is represented from various sources. Of the different Levels of Conceptual Interoperability Models, a level three is appropriate for this study, as the internals of the system interface are not intended to be accessed by infrastructure managers (users). However, the details of internal functions will be accessible to the Sim Center, which is in charge of designing the system.

Two general types of data will circulate the system: (1) BIM models of the infrastructures and buildings in the city; and (2) performance data retrieved by smart sensors. Note that each infrastructure has its specific type of sensors and has a distinctive set of performance data. For instance, the performance data that are collected from a bridge might be of a different nature than the ones collected from a power plant. However, to enable interoperability, the smart sensors are required to collect data in standard format and order, as defined by the National Institute of Standards and Technology, and in the ASCII encoding with blank separated values.

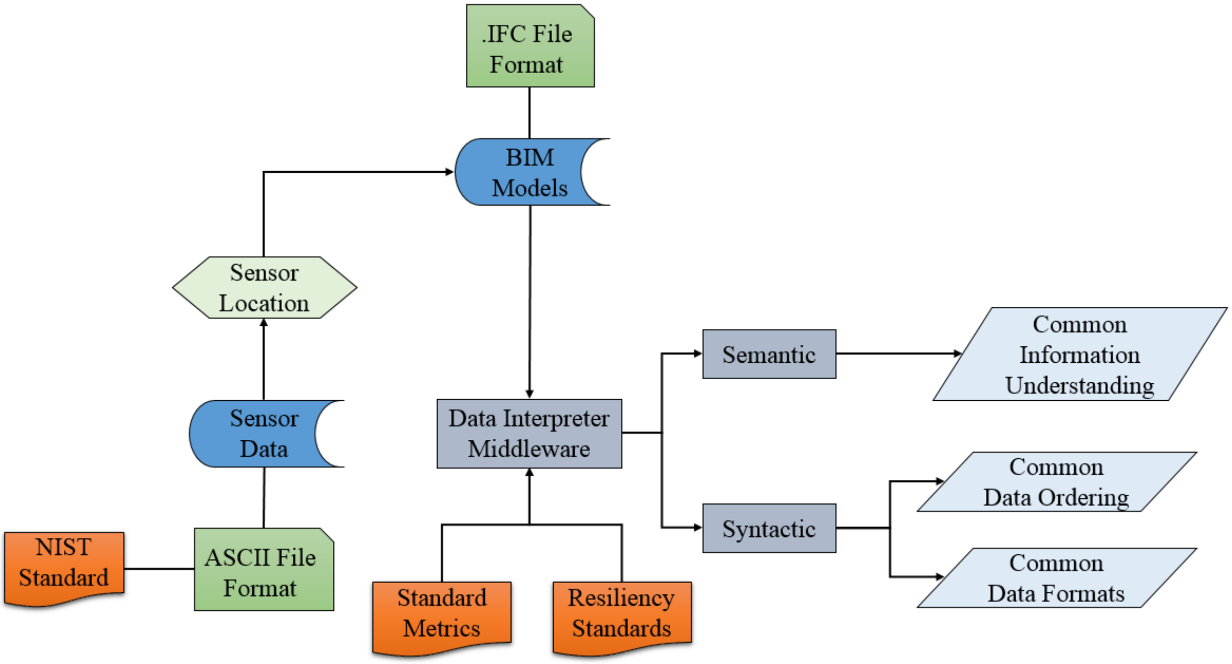
BIM models and sensors are integrated and communicate with each other once the sensor's location is identified by the BIM model using the "sensor_ID" attribute, which is unique and acts as a primary key for the sensor. Once the BIM model is augmented with sensor performance data, it is sent to the server at the Sim Center. A sample integration of a bridge girder's sensor with a BIM model through an XML interface is presented in Figure 8. Then, a data interpreter middleware completes the process of interoperability by enabling semantic and syntactic interoperability. The middleware goes over the data and converts the values to a standard metric system that is initially mandated by the system's interoperability guidelines. The output is a representation of the data that is understandable by computing components and has the required common ordering and format. This process also enables cross-domain interoperability since data from multiple types of civil infrastructures are classified and organized in a common framework. Figure 9 summarizes the process that makes the SoS interoperable at the information level.

Figure 8. XML Schema for Integration of a Bridge Girder's Sensor with the Girder's BIM Model



```
<?xml version="1.0"?>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">

 <xsd:element name="bridge_girder">

  <xsd:complexType>

    <xsd:sequence>

     <xsd:element name="bridge_girder" minOccurs="1" maxOccurs="unbounded">

        <xsd:complexType>

          <xsd:sequence>

                    <xsd:element name=“Girder_type" type="xsd:string" minOccurs="1" maxOccurs="1"/>

                    <xsd:element name="Girder_ID" type="xsd:string" minOccurs="1" maxOccurs="1"/>

                    <xsd:element name="Girder_Manufacturer" type="xsd:string" minOccurs="1" maxOccurs="1"/>

                    <xsd:element name="Location_in_the_Bridge" type="xsd:float" minOccurs="1" maxOccurs="1"/>

                    <xsd:element name="Allowable_Stress" type="xsd:float" minOccurs="1" maxOccurs="1"/>

                    <xsd:element name=“Sensor_ID" type="xsd:string" minOccurs="1" maxOccurs="1"/>

                    <xsd:element name="Sensor_Current_Detected_Load" type="xsd:float" minOccurs="1" maxOccurs="unbounded"/>

                    <xsd:element name="Sensor_Current_Detected_Deflection" type="xsd:float" minOccurs="1" maxOccurs="1"/>

        </xsd:sequence>

       </xsd:complexType>

     </xsd:element>

    </xsd:sequence>

  </xsd:complexType>

 </xsd:element>

</xsd:schema>
```

Figure 9. Information Interoperability for Resilient Civil Infrastructures SoS



5. Testing

The proposed SoS must be tested at different integration levels to verify that the defined requirements are met. Specifically, the proposed SoS requires validation for several use cases, especially at the acceptance stage using synthetic performance data and historical multi-hazard event information. The system must be tested with sets of defined scenarios using a simulation-based technique for validation purposes. For instance, suppose the system diagnoses that a particular civil infrastructure has required resiliency for an earthquake with a specified magnitude. The effect of an earthquake on the infrastructure must be simulated to validate the accuracy of the system's diagnosis.

The SoS integration is tested using a bottom-up approach by testing from the lowest level units, such as sensors, to infrastructure, and eventually to the complete system level. A sample black-box test module is presented in Table 2. The objective of the test is to verify that the sensor network connection works at a satisfactory level, meaning that the sensors can effectively connect to routers and eventually to the server. The received signal's strength and data transfer frequency is recorded along with the time it takes for the server to receive the data. Various types of sensors are tested and their connection to routers is verified. It is assumed that signal strengths are lower than 55 dB, data transfers less than 1 per minute, and that average transfer times are below 0.5 milliseconds.

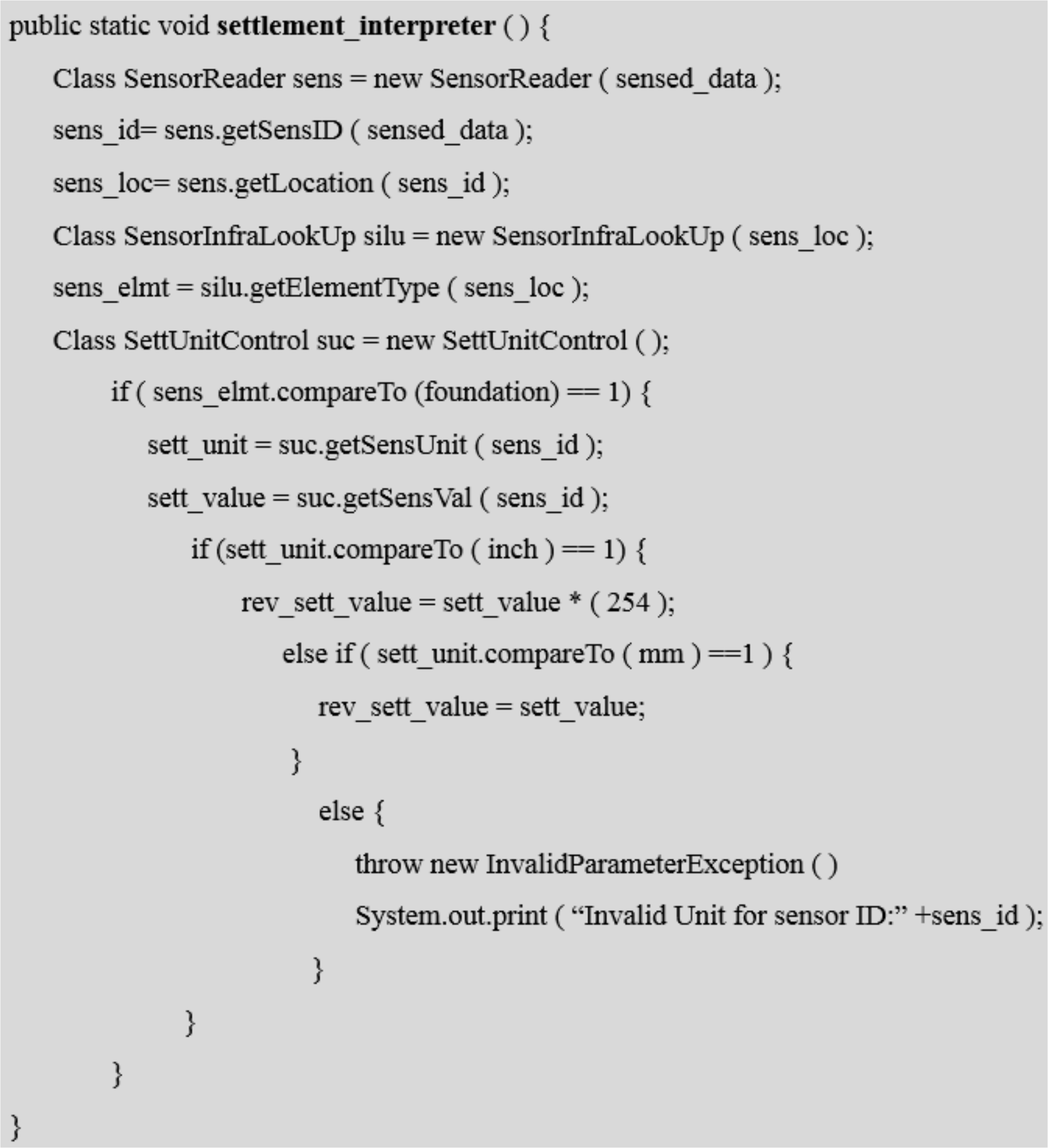
Table 2. Sample Black-Box Test to Verify Connection in Sensor Network

Sensor ID	Router ID/Distance from Router (m)	Received Signal's Strength (dB)	Data Transfer Frequency (per min)	Avg. Transfer Time (ms)
BR_1050	RBR_001, 3	56	0.5*	0.5
BR_1070	RBR_002, 5	55	1	0.4
BR_1090	RBR_002, 2	59	1	0.35
BR_1110	RBR_003, 7	54*	1	0.55*

A set of white-box tests shall also be designed to ensure the software internals work properly. These tests shall be designed specifically to verify the integrity of the software components that run queries or perform computations and resiliency analysis. These tests are also critical from a system validation perspective because achieving the final goal, which is the resiliency of civil infrastructures, depends to a significant degree on the accuracy of the computations and algorithms at the bottom level of software internals.

A sample white-box test inspects the code that is used to enable interoperability at the middleware of the Sim Center's server (refer to Section 4). The code's logic is as follows. The code receives data from a sensor, detects the sensor ID, and identifies the type of infrastructure that the sensor belongs to by using the location of the sensor, which is represented by coordinates. Next, it finds the type of structural elements to which the sensor is attached. Suppose that the interoperability guidelines mandate that foundation settlements must be presented in millimeter units while some of the sensors produce data in inches. The code retrieves the data and, if it was related to a foundation, it converts the sensed data to millimeters. To test the software internals, the code is fed with different formats of data to verify that the middleware converts them to the appropriate data formats. Error handlings and exception handlings must be tested as well. For instance, in the following sample, the code should throw an exception and notify the human operator if the sensed data's format is not recognizable by the code.

Figure 10. An Object-Oriented Programming Method that Ensures Sensed Data Have Common Unit of Millimeter



```
public static void settlement_interpreter ( ) {
    Class SensorReader sens = new SensorReader ( sensed_data );
    sens_id= sens.getSensID ( sensed_data );
    sens_loc= sens.getLocation ( sens_id );
    Class SensorInfraLookUp silu = new SensorInfraLookUp ( sens_loc );
    sens_elmt = silu.getElementType ( sens_loc );
    Class SettUnitControl suc = new SettUnitControl ( );
          if ( sens_elmt.compareTo (foundation) == 1) {
              sett_unit = suc.getSensUnit ( sens_id );
              sett_value = suc.getSensVal ( sens_id );
                  if (sett_unit.compareTo ( inch ) == 1) {
                        rev_sett_value = sett_value * ( 254 );
                            else if ( sett_unit.compareTo ( mm ) ==1 ) {
                                rev_sett_value = sett_value;
                             }
                                else {
                                    throw new InvalidParameterException ( )
                                    System.out.print ( “Invalid Unit for sensor ID:” +sens_id );
                               }
                  }
          }
}
```

6. Legacy System's Integration

Two main legacy systems need to be integrated into the proposed SoS: (1) the legacy information system of CAD documents; and (2) the legacy system of infrastructure performance monitoring which is based on fragmented sensors that usually require manual effort for data interpretation. The plan is to transition from these legacy systems to a comprehensive set of BIM models for infrastructures at the city level, as well as an infrastructure-level wireless sensor network system for the collection of infrastructure performance data.

The current CAD system can be used to generate 3D BIM models. Since the existing operations of infrastructures are dependent on the traditional CAD system, a gradual migration type of integration is recommended. The integration approach should be designed such that the existing operational processes are not disrupted while transitioning to the new system; therefore the transition should be a combination of cut-and-run and phased interoperability. The cut-and-run approach should be used for the components of the legacy system that have a minimal effect on its operation. The CAD legacy system should be gradually replaced with a building information model-based system. The traditional interfaces should be dismantled and replaced with new web-based interfaces. Human operators should be trained to use the new interfaces while the transformation is taking place to decrease human-web-interface issues.

As discussed earlier in the paper, different civil infrastructure systems within the city should be represented as nodes of the city's infrastructure network. The main framework of the new SoS should be designed and implemented, however, not all the infrastructure systems (nodes) should be connected to it at the same time as some of them are legacy systems and, as such, need improvements before joining the network. As the BIM models are generated and sensing systems are installed at different nodes, they gradually integrate with the new system until the entirety of the old system is replaced by the new one.

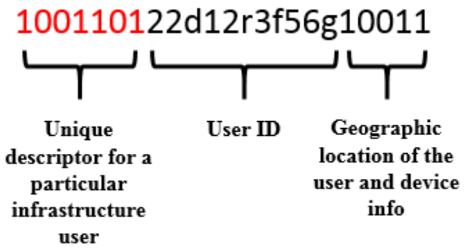
For the wireless sensor network system, a parallel operation will be used. The infrastructure owners currently manage, monitor, and operate the infrastructures with legacy systems and, therefore, a cut-and-run is neither practical nor reasonable. Instead, a parallel operation type of integration will be used, so that the old system continues to operate while the new system is being set up. Once the sensor is installed and its connections are established, the new system will be tested and, if the results are satisfactory, it will take over.

7. Cybersecurity

The proposed SoS works on the basis of heavy data transactions that contain sensitive information about critical infrastructures of a city. Cybersecurity plays a very important role. Several entities are interested in penetrating the system to access critical information and take control of the infrastructures to cause destruction. Among such potential threats are criminal organizations, foreign intelligence services, terrorists, hackers, spyware, and malware. The fact that infrastructure databases are connected to the centralized data warehouse through a cloud system makes it even more important to protect the system from intruders. To prevent unauthorized external access to the system and its data, system users should communicate through secured connections and IP addresses. Moreover, a real-time online tracking module is required to track the online users of the system and monitor their activities in order to detect suspicious activity.

An Artificial Immune System (AIS) integration is proposed in this paper to enforce authorized access to the system and prevent security breaches. Authorized users of the system are generally categorized as human operators in the infrastructures and operators at the Sim Center. Each infrastructure has a closed-network local connection with unique IP addresses that are specific to the infrastructure and the Sim Center since they have direct communication. Note that the Sim Center is designed as a communication hub and, therefore, every communication between two infrastructures must go through the Sim Center portal. This would decrease communication flexibility but at the same time increase the security of the system and limit the possibility of security breaches.

To design the security system, first we must recognize the requirements of the system users (also known as "self") in terms of the types of accesses and inquiries. For instance, authorized actions for an infrastructure operator include access to sensor data to review their status, review the energy efficiency of the infrastructure, etc. A negative selection algorithm is adopted as the main discriminator method for the system. Infrastructure and Sim Center operators will each have a unique descriptor that distinguishes them from each other. At the same time, every authorized user of the system has a unique ID which is represented as a set of numbers and is attached to the unique descriptor of the user. For instance, a user's string for infrastructure would look like the following:


1001101 22d12r3f56g 10011
Unique descriptor for a particular infrastructure user
User ID
Geographic location of the user and device info

The last set of numbers indicates the geographical location and the IP address of the device with which the user is identified. The censoring phase of the AIS system is comprised of the generation of random sets of strings that are similar to the one presented above. If a string is generated that is not similar to the string of an infrastructure operator, then the string is designated a detector. The detector set is then used to identify non-selves. However, the different types of strings that are active in the system must be continuously monitored. Authorized actions are attributed to the "self" strings and, the censoring phase would consider activities in the filtering process. There are generally three types of breach that could happen in the system: (1) a user takes an unauthorized action; (2) an intruder tries to penetrate the system but does not have access to any system users' info; and (3) an intruder replicates a system user's ID to remain unrecognizable. To detect these breaches, robust activation and adaptive thresholds must be defined to handle single attacks as well as coordinated, multi-host attacks. These thresholds are especially useful in the prevention of the third type of breach, in which an intruder might manage to steal the credentials of a user for unauthorized activities. The first feature that is detected by the detectors is whether the last five digits of the user's strings correspond with the registered geographic and device information of the user. If the last digits do not match, the system raises an alert that causes the system to validate the identity of the user before authorizing any action.

However, this detection is not sufficient if an intruder manages to replicate a user's string. To tackle this problem, a learning component is added to the system. This component has the capacity to learn the pattern of actions taken by users and detect anomalies. In cases in which it detects an anomaly, the system immediately blocks any action in progress. This learning component also improves itself by learning from previously generated false and true alarms. However, this must not lead to an adjustment of the system that could be advantageous to intruders. A conservative thresholding method must be applied to prevent this.

The censorship phase in the negative selection algorithm must be augmented with a process that can generate encrypted strings to make it unpractical for an external system to generate strings similar to the ones defined for the infrastructure operators. In addition, a hacker might program malware that would make the censoring phase filter out non-self-strings and detect them as self—this is similar to the situation in which the body's immune system attacks itself instead of defending the body. Therefore, there must be a monitoring system assigned to the censorship phase to detect anomalies in the process.

Finally, an Affinity Maturation Learning mechanism must be implemented so that different detectors would compete to identify non-selves. This would not only decrease the false alarm rates but would also improve the general security of the system since multiple detectors would be engaged in the process. A proper threshold distance metric must be implemented. Since the defined strings have a binary nature (except the part comprised of a user ID), a Hamming distance would be appropriate to compute which detector has the closest match.

8. Conclusion

This paper provides a study on SI methods for the resiliency of civil infrastructure systems for multi-hazard events. It models the problem using an SoS approach and develops the related integration ontology. The proposed SoS's performance depends heavily on the implementation of a comprehensive interoperability guideline and relevant integration methods. This study focuses on integration at the city level, however, the system boundary could be expanded to the national level as well. The proposed SoS operates based on state-of-the-art data sensing technologies and uses integration resources such as ubiquitous computing and artificial intelligence. The paper emphasizes increasing the resistance and absorbability of civil infrastructures by continuously monitoring their resiliency condition. The benefits of the proposed SoS could be extrapolated to decision-making processes in post-disaster stages to facilitate the recovery period of civil infrastructure systems.

Bibliography

[1] Zimmerman, Rae, and Carlos E. Restrepo. 2009. "Analyzing Cascading Effects within Infrastructure Sectors for Consequence Reduction." In *2009 IEEE Conference on Technologies for Homeland Security*, 165–70.

[2] Reed, Dorothy, Zelda Zabinsky, and Linda Boyle. 2011. "A Framework for Optimizing Civil Infrastructure Resiliency." In *2011 Structures Congress*, 2104–12.

[3] Chang, Stephanie E., Timothy L. McDaniels, and Dorothy Reed. 2005. "Mitigation of Extreme Event Risks: Electric Power Outage and Infrastructure Failure Interactions." In *The Economic Impacts of Terrorist Attacks*, edited by Harry. W. Richardson, Peter Gordon, and James E. Moore II. Edward Elgar Publishing.

[4] Madni, Azad M., and Michael Sievers. 2014. "Systems Integration: Key Perspectives, Experiences, and Challenges." *Systems Engineering* 17 (1): 37–51.

[5] Bruneau, Michel, Stephanie E. Chang, Ronald T. Eguchi, George C. Lee, Thomas D. O'Rourke, Andrei M. Reinhorn, Masanobu Shinozuka, Kathleen Tierney, William A. Wallace, and Detlof von Winterfeldt. 2003. "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities." *Earthquake Spectra* 19 (4): 733–52.

[6] Bocchini, Paolo, Dan Frangopol, Thomas Ummenhofer, and Tim Zinke. 2014. "Resilience and Sustainability of Civil Infrastructure: Toward a Unified Approach." *Journal of Infrastructure Systems* 20 (June): 04014004.

[7] Ouyang, Min, and Leonardo Dueñas-Osorio. 2011. "Resilience Modeling and Simulation of Smart Grids." In *2011 Structures Congress*, 1996–2009.

[8] Mostafavi, Ali, Dulcy M. Abraham, Daniel DeLaurentis, and Joseph Sinfield. 2011. "Exploring the Dimensions of Systems of Innovation Analysis: A System of Systems Framework." *IEEE Systems Journal* 5 (2): 256–65.

[9] Mostafavi, Ali, and Dulcy M. Abraham. 2014. "Resilience-Based Planning in Civil Infrastructure Using System-of-Systems Analysis." In *Construction Research Congress 2014*, 1249–58.

[10] Brownjohn, James, and Emin Aktan. 2013. "Improving Resilience of Infrastructure: The Case of Bridges." In *2013 Structures Congress*, 1812–21.

[11] Office of the Deputy Under Secretary of Defense for Acquisition and Technology. "Systems Engineering Guide for Systems of Systems." Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering, Washington, DC: ODU.S.D(A&T)SSE2008.

About the Author

Vahid Balali, PhD

Dr. Balali is the principal investigator and an Associate Professor in the Department of Civil Engineering and Construction Engineering Management at California State University Long Beach. Dr. Balali's research focuses on visual data sensing and analytics, virtual design and construction for civil infrastructure and interoperable system integration, and smart cities in transportation for sustainable decision-making.

Dr. Balali is a recipient of the 2020 Early Academic Career Excellence Award from California State University Long Beach. He was also selected as one of the Top 40 under 40 by the Consulting-Specifying-Engineer for the year 2017 and the top young professional in California by the Engineering News-Record for the year 2016. He received the 2014 second-best poster award from the Construction Research Congress, as well as the 2013 CMAA national capital chapter scholarship award. He is currently an associate member of ASCE and CMAA, a committee member of the ASCE Data Sensing and Analysis and ASCE Visual Information Modeling and Simulation committees, and a friend member of relevant TRB committees. He is also serving as a reviewer of several top journals. He is actively collaborating with industrial partners and is involved in professional and outreach activities.

MTI FOUNDER

Hon. Norman Y. Mineta

MTI BOARD OF TRUSTEES

Directors

MTI
MINETA
TRANSPORTATION
INSTITUTE