A conceptual model and proposed solution for analyzing Information Quality for Critical Infrastructures

MOHAMAD GHARIB, PAOLO LOLLINI, ANDREA BONDAVALLI

University of Florence, Italy
mohamad.gharib@unifi.it

Keywords: Critical Infrastructures, System-of-Systems, Information Quality

Our society heavily depends on various interdependent Critical Infrastructures (CIs), where their disruptions may result in significant consequences for the society as a whole. Therefore, their dependability is a main concern to both governments and citizens. Information plays a key role in the coordination, cooperation, and collaboration of interdependent activities of CIs. In this context, such information should be of proper quality in order to guarantee a proper interdependency among CIs. As an increasing number of researchers are dealing with CIs as a System of Systems (SoS), we adopt our conceptual model for analyzing Information Quality (IQ) for SoS and apply it to the case CIs. We illustrate the applicability of the model for analyzing IQ for CIs by applying it to a realistic example concerning a cooperative road infrastructure system for driver overtaking assistance.

1. Introduction

Nowadays, our society depends heavily on various infrastructures such as electricity grids, telecommunications, oil and gas pipelines, transportation, banking and finance, emergency and government services, agriculture systems etc. [1,2]. Some of these infrastructures such as transportation, electrical distribution, water supply, and telecommunications systems provide essential services to our society, therefore and due to their importance they are often characterized as Critical Infrastructures (CIs) [2]. More specifically, CIs are those systems that are so vital to citizens and economy, where their disruptions may result in significant consequences for the society as a whole [2]. For example, the transportation infrastructure is of crucial importance for any country, where the majority of the population depends on its facilities on a daily basis [3].

The proper functioning (dependability) of CIs is always a main concern to both governments and citizens. The importance of CI dependability has been highlighted by many researchers [4], and it has also emerged out by several events (e.g., Galaxy 4 failure [1], Hurricane Sandy [5]). However, current CIs do not operate in isolation [4], they are highly interconnected and interdependent in complex ways [1,4], where such interdependencies can be physical, cyber, geographical, or even logical [1]. This makes maintaining their dependability even harder since a failure in one CI may propagate to other CIs [1], and potentially resulting in cascading effects that impact all aspects of society [4,5]. Recent disasters, such as the Fukushima earthquake and the Hurricane Sandy, have demonstrated the significant consequences of CIs failure [5].

Information plays a key role in the coordination, cooperation, and collaboration of the interdependent activities of CIs. Therefore, such information should be of proper quality in order to guarantee a proper interdependency among CIs [2]. On the other hand, increasing number of researchers are refereeing to CIs as a System of systems (SoS), whose function depends on the performance of individual complex systems [1,6]. The role of information in integrating the systems of SoS has been discussed by several researchers (e.g., [7]), but they did not consider the quality of such information. This leaves the system open to depending on inaccurate, incomplete, inconsistent, invalid, untrustworthy information, which may result in undesirable outcome or it may even lead an overall SoS failure [8]. To this end, we adopt our conceptual model for analyzing Information Quality (IQ) for SoS, and we illustrate its applicability for analyzing IQ for CIs.

The rest of this paper is organized as follows. Section 2 describes a motivating example. In Section 3 we discuss our conceptual model for analyzing IQ for SoS, and we illustrate its applicability for analyzing IQ for CIs in Section 4. Finally, we conclude in Section 5.

2. Motivating example: cooperative driver overtaking assistance

Our example concerns a cooperative road infrastructure system that aims at supporting drivers while overtaking on two-lane roads. Overtaking on two-lane roads is a difficult driving task, and relatively high number of traffic fatalities (35-50%) are directly related to passing/overtaking maneuvers [9]. Therefore, a system that is able to assist drivers to avoid takeover-related accidents is required. However, it is not easy to design such complex system with stand-alone solutions [10]. Thus, a cooperative road infrastructure system is required, where road surface based units, vehicles, and other road infrastructure cooperate to solve this problem [10]. The proposed system is based on existing literature [9,10], and its main components can be classified under:

- Road Marking Units (RMUs) are integrated into road infrastructure, and they collect and disseminate information that assists drivers to avoid takeover-related accidents.
- Drivers/vehicles aim to reach their destinations safely, which implies avoiding takeover-related accidents.

While for communication channels in the system, we differentiate between two types:

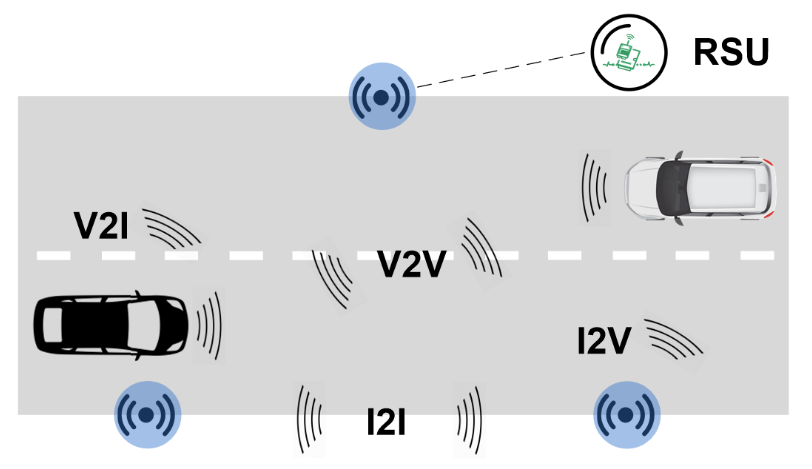
1. Direct channels:
   - *RMUs-to-RMUs* (Infrastructure-to-Infrastructure/I2I): allows RMUs to communicate with one another to exchange information.
   - *RMUs-to-Vehicle* (Infrastructure-to-Vehicle/I2V): allows RMUs to communicate with vehicles.
2. Indirect channels (stigmergic channels [8]):
   - *Vehicle-to-Vehicle*/V2V: allows vehicles/drivers to collect (sense) information (e.g., location, direction etc.) about other vehicles.
   - *Vehicle-to-RMUs*/V2I: allows RMUs to collect information about passing vehicles.

Figure 1 shows a partial diagram of the system in terms of its main components along with their direct and indirect communication channels.

3. A conceptual model for analyzing Information Quality for System of Systems

IQ refers to how well information meets the requirements of its consumers, which can be analyzed through various IQ dimensions [11]. Several models for analyzing IQ based on its different dimensions have been proposed in the literature (e.g., [11,12]). However, none of them consider information that is exchanged through stigmergic channels, which make them inappropriate for analyzing IQ for SoS. To tackle this problem, we have proposed a conceptual model specialized for analyzing IQ for SoSs in terms of four core IQ dimensions [8], namely accuracy, completeness, timeliness and consistency. In this model, the real world is made up of *things*, where each *thing* has a *state* that has a set of *state variables*. *Things* can be represented in Information System (IS) by *information objects,* and each *of them* has a set of *produced information.* A couple of a *state variable* and a *produced information* that represent it are called a corresponding couple, and the value of each *produced information* should reflect the value of its corresponding *state variables*.

Figure 1.
A partial diagram of the cooperative assistance system



A SoS integrates a number of *Constituent Systems (CSs)*, which can be either *intentional* or *unintentional CSs.* A *CS* can *produce information (produced information)* by *acquiring* its *value* from its corresponding *state variable*. While *Intentional CSs* can *create* information *(created information).* A *CS* can *send/receive messages* that *contain information* by *relying* on *message interface, which transmits* messages depending on a *channel.* Moreover, a *CS* can *perform activities* that can be either *Intentional or Unintentional communicative activity,* where the first are performed with the intention of changing a *state* of a *thing* to convey a *message*, and the last are not performed to communicate any information.

In this model, we analyzed the *accuracy of produced information* by comparing its *value* with the *value* of its corresponding *state variable.* While the *accuracy of created information* is analyzed based on the trustworthiness of its (i) source (*trusted,* distrusted, or *unclassified CSs*), (ii) the type of activity that produces such information (*legitimate, suspicious,* or *malicious*), and (iii) information content (*safe, potentially harmful,* or *harmful*).

Moreover, we analyzed the *completeness* of *information* depending on: 1. *Value completeness,* information is value *complete* if it has been transmitted through an integrity-preserving channel, otherwise it might not be. 2. *Purpose of use completeness,* information item should have all its parts for performing a specific activity. This analysis can be performed depending on three concepts, namely *part_of, purpose of use* and *relevant_to.*

For analyzing the *timeliness of produced information,* we compare its *volatility* with the *real volatility* of its corresponding *state variable,* and information is valid if they are close enough, and otherwise, it is out-dated. While *created information timeliness* is analyzed by comparing its *use-time* with its *validity time,* if its *use-time* is less than its *validity time,* information is valid, otherwise, it is not. Finally, we analyzed *information consistency* depending on several concepts such as *interdependent activities* that are *activities* belong to the same *activity type,* and per-

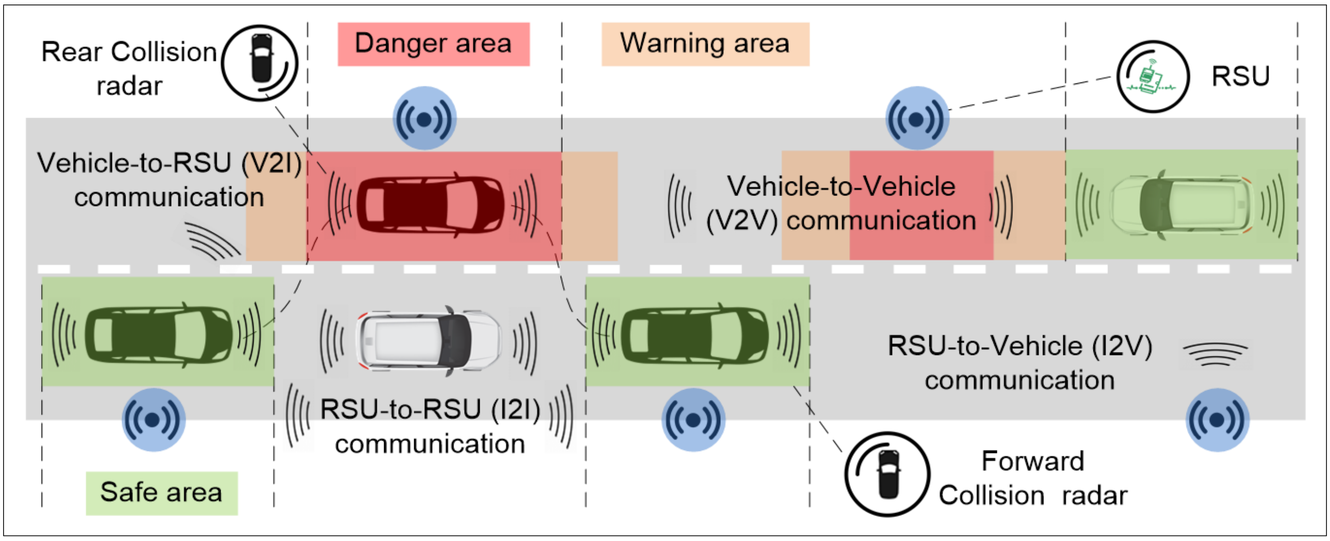

Rear Collision radar
Danger area
Warning area
RSU
Vehicle-to-RSU (V2I) communication
Vehicle-to-Vehicle (V2V) communication
RSU-to-Vehicle (I2V) communication
RSU-to-RSU (I2I) communication
Safe area
Forward Collision radar

Figure 2. A partial diagram of the cooperative overtaking assistance system with the critical zones

formed in the same *Sphere of Action (SoA),* which is a partial part of the domain. While CSs who are performing *interdependent activities* are called *interdependent CSs,* and inconsistency result from providing/updating information used by *interdependent CSs* with different delay time/update rate.

4. Illustrating the applicability of our model for analyzing IQ for CIs

In this section, we illustrate the applicability of our conceptual model for analyzing IQ for CIs. According to Birk et al. [10], overtaking in two-lane roads consists of four main phases: (i) the driver estimates the possibility of safely overtaking a lead vehicle, (ii) the driver initiates the overtaking, (iii) the driver passes the lead vehicle in the opposite lane, and (iv) the overtaking is completed by changing the lane back into the original lane of the vehicle. Taking these four phases of an overtake in mind, vehicles can be in one of three main areas: (i) safe area (green), the vehicle is safe with respect to any danger that might result from an overtake; (ii) warning area (orange), the vehicle can be in danger due to an overtake in process; and (iii) danger area (red), the vehicle can be in an imminent danger due to an overtake in process. *Figure 2* shows a partial diagram of the system along with the different critical zones.

Now let us consider for example a driver named Paolo, who is driving on two-lane road and aims to reach his destination safely. In order to „avoid takeover-related collision", Paolo needs to depend on takeover-related information, which can be obtained either from nearby RMUs[1] *(a trusted source)* or other vehicles *(untrusted source since they may* disseminate false information [8]) using the same route. In this context, Paolo needs to depend on RMUs for acquiring *accurate* takeover-related information, since RMUs are classified as *trusted CSs* for such information, the activities that produce such information is *legitimate,* and the information content is *safe*.

On the other hand, in order to provide complete *takeover-related* information, RMUs need to depend on adjacent RMUs for information about incoming vehicles on the same lane, and on nearby RMUs that is located on the other side of the road. More specifically, such information is *relevant_to* the *purpose* of Paolo's *activity* (e.g., „avoid takeover-related collision"). Therefore, both of them are considered as sub-parts *(part_of)* of the *takeover-related* information, i.e., if any of them were not made available to Paolo, the *takeover-related* information will be considered incomplete for the *purpose of use.*

In order to avoid depending on *invalid* (out-dated) information, information should be updated with respect to the position and speed of the car, i.e., the driver should be notified within a period that enables him/her to take the right action to avoid an imminent accident. In other words, RMUs need to update the *value* of the *takeover-related* information among each other along with passing vehicles taking into consideration the *volatility* of the *value* of its corresponding *state variables,* i.e., the position and speed of subject vehicles. Note that different areas (green, orange, or red) have different timeliness updating requirements depending on their criticality.

Finally, to guarantee that vehicles will coordinate their activities appropriately in the subject area (e.g., takeover), they need to depend on consistent information. For example, when Paolo (or another driver of the opposite lane) starts initiating a takeover, RMUs should start notifying all vehicles trying to "avoid takeover-related collision" (interdependent activities) in the subject area (SoA), and this information should be consistent among all of these vehicles (interdependent CSs) in order to avoid a possible collision.

[1] *Note that RMUs depends also on both electrical and communication infrastructures, but to simplify the scenario we will mainly focus on the different interdependencies among RMUs and vehicles.*

5. Summary

In this paper, we advocated that IQ plays a key role in the performance of interdependent CIs. Moreover, we presented a conceptual model for analyzing IQ for SoS in terms of the four core IQ dimensions, and we illustrated its applicability for analyzing IQ for CIs by applying it to a realistic example, namely cooperative road infrastructure system for driver overtaking assistance.

Acknowledgment

This work has been partially supported by
the “Schema concettuale, metodologia e sua applicazione per la costruzione di Sistemi di Sistemi (Systems of Systems) cyber-fisici, self-aware e semi-autonomi” project,
and by the PIRSES-GA-2013-612569 DEVASSES project.

Authors

MOHAMAD GHARIB is a postdoctoral researcher under the supervision of Prof. Andrea Bondavalli at the University of Florence. Previously he was a postdoctoral researcher under the supervision of Prof. John Mylopoulos at the Department of Information Engineering and Computer Science, University of Trento, Italy, where he obtained his PhD degree in April 2015, under the supervision of Prof. Paolo Giorgini. His PhD work mainly focused on modeling and reasoning about Information Quality requirements for Socio-technical Systems (STS). His current research interests focus mainly on the modeling and analysis of Cyber-Physical System of Systems (CPSoS), with special emphasis on three main areas: 1. Information Quality, 2. Functional Safety Requirements and 3. Privacy Requirements.

PAOLO LOLLINI received the PhD degree in computer science from the University of Florence, Italy, in 2005. Since 2006, he worked as research associate at the same University, and he is currently an Assistant Professor at the Mathematics and Computer Science Dept. He has been continuously participating in European and National funded projects since 2002 up to present, including the recently concluded projects ICT-FP7-610535 AMADEOS, ARTEMIS-JU-333053 CONCERTO and PRIN-20103P34XC TENACE (National), and he is currently participating to the PIRSES-GA-2013-612569 DEVASSES project. He was a member of the program committee of important conferences in the area of dependable systems, including DSN, HASE, LADC, SRDS and currently EDCC. His current research interests include the stochastic modeling and evaluation of performability and resiliency attributes of large-scale critical infrastructures and systems of systems, with reference to a variety of application fields including railway, mobile telecommunications, and electric power systems.

ANDREA BONDAVALLI is a Professor of Computer Science at the University of Firenze. Previously he has been a researcher and a senior researcher of the Italian National Research Council, working at the CNUCE Institute in Pisa. His research activity is focused on Dependability and Resilience of critical systems and infrastructures. In particular, he has been working on safety, security, fault tolerance, evaluation of attributes such as reliability, availability and performability. His scientific activities have originated more than 220 papers appeared in international journals and conferences. Andrea Bondavalli led various national and European projects and participates in (and has been chairing) the program committee in several international conferences in the field. He is the chair of the Steering Committees of IEEE SRDS and a member of the editorial board of the International Journal of Critical Computer-Based Systems. Andrea Bondavalli is a member of the IEEE, the IFIP W.G. 10.4 Working Group on “Dependable Computing and Fault-Tolerance”.

References

[1] C. DeMarco, T. K. Kelly, J. P. Peerenboom, M. Amin, M. Ilic, and F. Alvarado,
“Critical infrastructure interdependencies (PANEL)”,
IEEE Winter Meet. Columbus, OH, 2001.

[2] B. Genge, I. Kiss, P. Haller, and C. Siaterlis,
“Generating high quality data for the protection of modern critical infrastructures”,
4th International Symposium on Digital Forensic and Security (ISDFS), 2016, pp.53–58.

[3] M. Gharib, P. Lollini, A. Ceccarelli, and A. Bondavalli,
“Dealing with Functional Safety Requirements for Automotive Systems: A Cyber-Physical-Social Approach”,
12th International Conference on Critical Information Infrastructures Security (CRITIS), 2017.

[4] P. F. Katina and C. A. Pinto,
“On critical infrastructure interdependency”,
Annu. Int. Conf. Am. Soc. Eng. Manag. (ASEM 2012), Agil. Manag. Embrac. Chang. Uncertain. Eng. Manag., October 2012, pp.29–38.

[5] A. Laugé, J. Hernantes, and J. M. Sarriegi,
“Critical infrastructure dependencies:
A holistic, dynamic and quantitative approach”,
Int. J. Crit. Infrastruct. Prot., 2015, Vol.8, pp.16–23.

[6] J. Jovel and R. Jain,
“Impact of Identified Causal Factors to ‘System of Systems’ Integration Complexity from a Defense Industry Perspective”,
Glob. J. Flex. Syst. Manag., 2009, Vol.10, no.4, pp.45–54.

[7] M. W. Maier,
“Architecting Principles for Systems-of-Systems”,
INCOSE Int. Symp., July 1996, Vol.6, no.1, pp.565–573.

[8] M. Gharib, P. Lollini, and A. Bondavalli,
“ A conceptual model for analyzing information quality in System-of-Systems”,
12th System of Systems Engineering Conference, SoSE 2017, 2017, pp.1–6.

[9] G. Hegeman, R. Van Der Horst, K. A. Brookhuis, and S. P. Hoogendoorn,
“Functioning and acceptance of overtaking assistant design tested in driving simulator experiment”,
Transp. Res. Rec., Dec. 2007, No.2018, pp.45–52.

[10] W. Birk, E. Osipov, and J. Eliasson,
“iRoad-Cooperative Road Infrastructure Systems for Driver Support”,
Proc. 16th ITS World, 2009.

[11] M. Gharib and P. Giorgini,
“Dealing with Information Quality Requirements”,
in International Conference on Enterprise, Business-Process and Information Systems Modeling, 2015, pp.379–394.

[12] M. Gharib and P. Giorgini,
“Modeling and Reasoning About Information Quality Requirements”,
in Requir. Engineering: Foundation for Software Quality, 2015, Vol.9013, pp.49–64.