A Multi-supplier Collaborative Monitoring Framework for Informatics System of Systems

Carlos Gonçalves, Tiago Dias, A. Luís Osório, Luis M. Camarinha-Matos

A Multi-supplier Collaborative Monitoring Framework for Informatics System of Systems

Carlos Gonçalves[1]; Tiago Dias[1,2]; A. Luís Osório[1]; Luís Camarinha-Matos[3]

[1]ISEL – Instituto Superior de Engenharia de Lisboa, IPL – Instituto Politécnico de Lisboa, and POLITEC&ID, Portugal, carlos.goncalves@isel.pt, tiago.dias@isel.pt, lo@isel.ipl.pt

[2]INESC-ID – Instituto de Engenharia de Sistemas e Computadores - Investigação e Desenvolvimento

[3]School of Science and Technology and UNINOVA-CTS, NOVA University of Lisbon Caparica, Portugal, cam@uninova.pt

Abstract. Managing interdependent cooperating informatics systems from multiple suppliers is a complex and challenging endeavor. Due to the lack of complete open standards, informatics systems from different suppliers are developed using incompatible protocols and programmatic interfaces (API). Often, incompatibilities also exist for informatics systems developed by the same supplier. Nevertheless, organizations must be able to monitor the systems that compose their Information Technology (IT) landscape transparently and independently of each system's supplier. This paper discusses a collaborative networks strategy associated with adopting the Informatics System of Systems (ISoS) framework for coordinated monitoring and support afforded by different supplying responsibilities. We argue that the adopted model simplifies the integration required by the digital, and makes efficient the collaboration among technology and service suppliers in supporting products' life cycle maintenance and evolution. Accordingly, we discuss the implementation of the proposed model in the HORUS project, which is motivated by the need to rethink a fuelling post-payment model of a petroleum company.

Keywords: Distributed Monitorization, Systems Integration, Collaborative Networks, Distributed systems.

1. Introduction

Organizations adopting informatics systems from different suppliers face several difficulties when managing integrated solutions. Although contemporary Information Technology (IT) systems are expected to incorporate informatics systems from multiple suppliers, each system exhibits its protocols and programming interfaces (API), often proprietary. Moreover, empirical evidence shows practices where tight collaboration with suppliers leads to tailored solutions with fuzzy responsibility borders. The statement of a representative executive officer of Hitachi [17] - "*... rather than delivering systems ..., what is needed is to hone solutions in partnership with customers ...*" - is a paradigmatic offering of a tailored approach. Such customized diversity of systems makes it very difficult and expensive to replace

existing monolithic and proprietary solutions with new or evolved systems showing equivalent capabilities from a competing supplier.

Furthermore, many of those monolithic proprietary systems are accountable for critical business processes that depend on computation services that rely on heterogeneous and interdependent complex systems. System elements need to be smarter and more cooperative in coping with the required reliability and resilience of the underlying technology. Approaches may range from a simple verification if a sub-system is available, e.g., reachable by a ping command, or a more complex inspection to infer performance metrics to check if technology elements are within a predefined set or ranges of values. Therefore, monitoring the health of specific technology elements that compose an organization's informatics systems landscape is challenging and of utmost importance for the reliability of the implemented services.

This paper presents and discusses a collaborative strategy for monitoring elements of informatics systems in a gas-fueling service area. The research problem relies on coordinating partial responsibilities when supplied by organizations with different processes and technology cultures. Our approach considers a collaborative strategy, challenging the participation of competing stakeholders collaboratively managing service failures and interdependencies. The proposed model also challenges the participation of the IT of the supporting stakeholder, since different systems on the provider's IT landscape need to interact with service elements of the informatics landscape of the fueling area. A simple example is the failure of a video camera on the responsibility of the Closed-Circuit Television (CCTV) maintainer company that compromises the vehicle identification service of the HORUS informatics system under the responsability of another company.

We validate the adoption of the Informatics System of Systems (ISoS) framework [11] as a strategy to move towards a Model-Driven Open Systems Engineering (MDEOS) vision and contribute to an open competitive technology market philosophy. The collaborative monitoring framework monitors services under the responsibility of different suppliers in the context of the HORUS research project [13]. The suggested strategy aims to support technology independence for the solution's owner and offers a basis for the recent trends on technology sovereignty [2] since the proposed approach reduces technology dependencies [11].

The remaining paper is organized as follows. Section 0 briefly presents the most prominent related research, the ISoS framework, and the HORUS project. Section 0 discusses the adoption of the ISoS framework to support the collaborative monitoring of the systems composing the HORUS project. Finally, Section 0 presents the conclusions and discusses future work.

2. Background

Monitoring is a long-discussed topic with contributions from complementary research perspectives ranging from technology to business. When observed from the computer distributed systems area, the research is more concerned with development issues, "*Monitoring supports the debugging, testing, and performance evaluation of computer programs*" [16]. Conversely, the communication networks have for long

contributed centered on networks reliability based on Simple Network Management Protocol (SNMP) and Network Management Stations (NMS) systems "…*the SNMP has two types of entities: managers and agents. Managers work in Network Management Stations and receive messages and traps from SNMP agents…*" [19]. Regardless of the approach, monitoring is gaining added attention with the evolving digital transition and the risks associated with the increasing diversity of technology artifacts that participate in the complex growth of the web of interdependencies. Moreover, the technology artifacts, being them communication infrastructure elements, cyber-physical systems, or software entities running on a cloud-based execution environment, public, private or hybrid, are critical for the proper support of people and businesses. This section briefly reviews the research work background, with Section 0.1 addressing the ISoS framework concepts and Section 0.2 revisiting the HORUS project.

2.1 The ISoS Framework

The ISoS framework [11] proposes a nonintrusive integration model to establish a multi-supplier or multi-vendor technology landscape to reduce the vendor lock-in risks, and ultimately be an enabler for technology sovereignty. The ISoS framework is based on three core modeling elements: `ISystem`, `CES`, and `Service`. The ISoS abstraction models the informatics landscape of an organization as a composite of one or more `ISystems`. An `ISystem` comprises one or more `CES`, whereas a `CES` consists of one or more `Services`. ISoS elements model the technology artifacts through a set of properties, e.g., name, version, supplier, or description. In the case of a `Service`, the modeling element instance has associated the metadata required for a peer *Service* to access the implemented functionalities. **Fig. 1** depicts the primary elements that make an organization ISoS enabled, using the SysML block syntax [6].

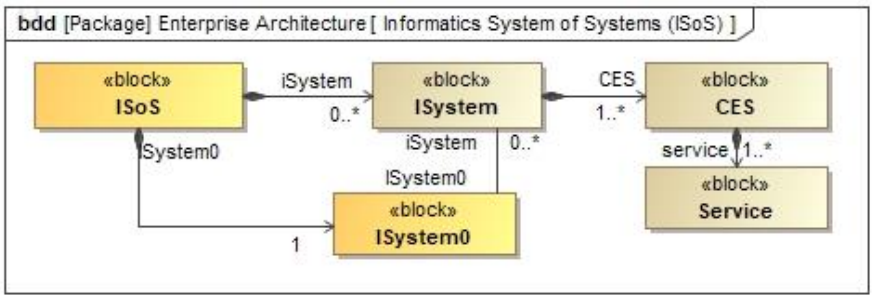

Fig. 1 – The simplified SysML block definition diagram of the ISoS model

The ISoS model considers a meta-*element* with management or coordination roles at the ISoS, `ISystem`, and `CES` levels, respectively, $\texttt{ISystem}_0$, $\texttt{CES}_0$, and $\texttt{Service}_0$. The initial reference implementation of the ISoS framework is based on the Java ecosystem. The proof-of-concept implementation further relies on the open-source Apache Zookeeper [7] to ensure that the ISoS metadata stored by $\texttt{ISystem}_0$

shows higher availability to the systems and services that compose the informatics landscape of an organization. A primary role of the $\texttt{ISystem}_0$ is to act as a directory service managing the metadata of the ISoS elements that exist within an organization, which we refer to as the Organization's computing-related technology artifacts (or Organization's information system). Accordingly, to be ISoS-enabled, an organization needs to instantiate, at least, the meta-`ISystem`, i.e., needs to hold running an instance of the $\texttt{ISystem}_0$, which has the unique role of managing the ISoS technology landscape. The ISoS framework model details are provided in [5].

2.2 The HORUS Project

The HORUS project was motivated by a real industry problem: how to improve the user experience in refueling vehicles by removing the (manual) pre-payment authorization procedure. Before HORUS, authorization had to be granted by the operator of the refueling area before a user could start to refuel the vehicle. This authorization typically involved manually checking an event list of vehicles with pending payments. Such lists used to be paper-based and very difficult to maintain and update with the aggregated information from all the refueling areas. Thus, the refueling areas without an automatic control of payments typically chose to operate in a pre-payment operation mode, demanding that the user had to pay before refueling.

The payment control with HORUS has simplified the refueling process. When a vehicle enters a refueling area, an image of the vehicle license plate is obtained and identified to produce a hash of its license plate. When the user removes the nozzle to fill the vehicle's tank, the payment console system presents a message to the operator to warn him about any pending payments for that vehicle. If there are pending payments, the operator may choose not authorize the refueling. Suppose a vehicle leaves the refueling area without paying. In that case, the hash of its license number is inserted in an events list stored by a persistence service available to all the refueling areas. The next time such a vehicle with a pending payment tries to refuel, the operator is shown a message to warn him about the faulty situation. In that case, the driver has to follow the pre-payment procedure until the payment issue is solved.

Although the rationale of the HORUS project is quite simple, its implementation involves heterogeneous systems implemented by different suppliers. Thus, the HORUS is an informatics system that uses other informatics systems, like the Point of Sale (POS) or the Closed-Circuit Television (CCTV) system responsible for the video cameras used by the License Plate Recognition (LPR) service used to identify the vehicles. The fact that the fueling network has its CCTV system under the responsibility of different companies introduces an added complexity to the management of monitoring events.

The above scenario clearly shows that the informatics systems landscape of a fuelling forecourt can be viewed as a network of different informatics and cyberphysical systems, each one with diverse responsibilities and that need to cooperate. Thus, it is imperative to provide a monitoring strategy based on anticipating reactions to any problem that might affect the several components of the HORUS that each service provider is responsible for. The strategic goal is to manage interdependent monitoring and maintenance responsibilities in a collaborative

network context. By collaborative monitoring and maintenance, we mean each participating stakeholder shall be aware of another participating stakeholder's failure and maintenance actions. In other words, from our previous research, it means that any informatics system has a tandem system we suffix by '-M' specialized to make effective monitoring and support maintenance processes [12].

3. The HORUS Project Case Study

Fig. 2 shows the different elements composing the informatics landscape of a forecourt gas station modeled by adopting the ISoS framework. Besides the $\texttt{ISystem}_0$, we can see the "HORUS" and the "CCTV" informatics systems, as well as the corresponding monitoring sub-systems, denoted by the labels "HORUS-M" and "CCTC-M", the tandem informatics system as discussed above.

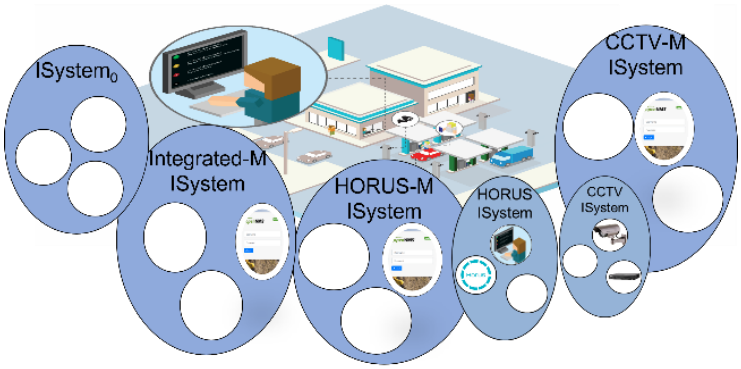

Fig. 2 – Elements involved in the HORUS project for a gas station forecourt

Different suppliers support the maintenance and evolution of the HORUS and the CCTV systems. Following the adopted model, monitoring and maintenance management must coordinate with supplier's informatics infrastructure. Thus, the integrated monitoring view of the forecourt gas station, denoted by the "Integrated-M" system, must work collaboratively with all the internal informatics and also with those of the suppliers. The remaining sections discusse how the ISoS framework is adopted to support the collaboration among the diverse technology elements, focusing on monitoring the participating related informatics systems. Section 0.1 discusses alternatives for supporting the monitoring systems, and Section 0.2 details the usage of the ISoS framework to support the collaboration between the elements of a forecourt and the collaborative network of support and maintenance providers.

3.1 Monitoring Systems

Monitoring plays a crucial role in an organization's multi-provider informatics technology landscape. Because an informatics technology landscape holds different types of systems and system elements, one may consider choosing alternative monitoring systems, each one better fitting a class of available parts. For example, we might consider a monitoring system to handle the IoT devices and another for monitoring the health of existing servers. However, this approach can quickly become infeasible if the Organization's amount and type of elements increase.

Monitoring solutions like ICinga [10], Nagios [1], and, more recently, OpenNMS [4], are systems aimed at monitoring the health of network elements such as routers and switches. The main idea behind these systems is that every network equipment has associated a Management Information Base (MIB), which can be seen as a modeling element representing the properties of the technology elements within a network of computers. The concept of a MIB is often associated with the Simple Network Management Protocol (SNMP) used by the monitoring systems to obtain the status/properties of the elements under monitoring. Other solutions like Zabbix [9] and Prometheus [18] target the monitoring of informatics systems, e.g., to verify if a system is responding or if some system metrics are within predefined values.

An hypothesis is to generalize SNMP-based monitoring to informatics systems, such as the case of applying it to a campus infrastructure [19] or enterprise servers [8]. If adopting SNMP, the selection of OpenNMS to monitor the state of any element (hardware or software) that composes the informatics landscape of an organization requires that any computational service implements an SNMP agent and the corresponding MIB interface. The approach taken in the HORUS project is to develop agents for the elements that initially were not SNMP enabled and use the OpenNMS solution to monitor both computational and cyberphysical elements involved in a forecourt gas station. For example, in the case of the cameras shared with the CCTV system, one agent was developed to read the state of the cameras using the Open Network Video Interface Forum (ONVIF) [14] and export that state information using a custom MIB. The adopted approach makes it possible to monitor legacy network of new informatics systems elements following a unified approach based on the SNMP protocol. While latencies introduced by the monitoring are not critical in the HORUS system, other application domains may require further validations, e.g., performance dimension as discussed in [8].

3.2 Collaborative Monitoring Using the ISoS Framework

A characteristic feature of the ISoS framework is its independence from any specific technological solution. ISoS framework offers simple mechanisms for service elements within an organization, hardware or software, to publish their associated metadata to the $\texttt{ISystem}_0$. The metadata supports the discovery of Service elements through the path `ISystem/CES/Service` elements. Thus, when a service S_A from system `A` needs to use the service S_B from system `B`, it just needs to contact the $\texttt{ISystem}_0$ and issue a lookup operation to obtain the metadata of service S_B.

The metadata registered in the $\texttt{ISystem}_0$ is composed of a set of XML documents, where there is an XML document associated to each `ISystem`, `CES`, and `Service`. Using the ISoS framework metadata is possible to have different services from distinct suppliers with additional responsibilities working together in a collaborative network. The collaboration is possible because services from collaborative organizations or suppliers can mutually find each other and interoperate based on the $\texttt{ISystem}_0$ canonical entry point and ISoS metadata facilities.

Additionally, the metadata can support a user interface capable of browsing organization elements and providing a unified view and introspection mechanisms. An example is the Service `SerUI` included in the ISoS $\texttt{ISystem}_0$ [5], which allows an administrator to browse all the `System`, `CES`, and `Service` elements that exist in the informatics system of an ISoS enabled Organization. The above mentioned Service `SerUI` is a simple service that collects and shows an organization's existing elements (`System`, `CES`, and `Service`). However, using the same logic, it is possible to implement a new system responsible for monitoring virtually all the elements within the Organization.

Since in an ISoS-enabled organization, informatics systems publish their metadata, it is possible to offer a dashboard showing the status of informatics systems. **Fig. 3** illustrates an interface view of a Synoptic of Things (SoT) framework [15, 16] showing the global state of the informatics systems in a forecourt gas station adopting the HORUS informatics system. The SoT framework uses the concept of widgets to support the interaction with the end-user. We call Widgets-IoT to such widgets, which are abstractions of hardware or software elements, e.g., a video camera device or a license plate recognition software. A Widget-IoT comprises common properties such as size, color or image. Also, specializations of Widget-IoT might contain properties for accessing a cyber-physical device. A Widget-IoT is a standard Web Component [3] making it possible to use Widgets-IoT in other contexts than the SoT framework.

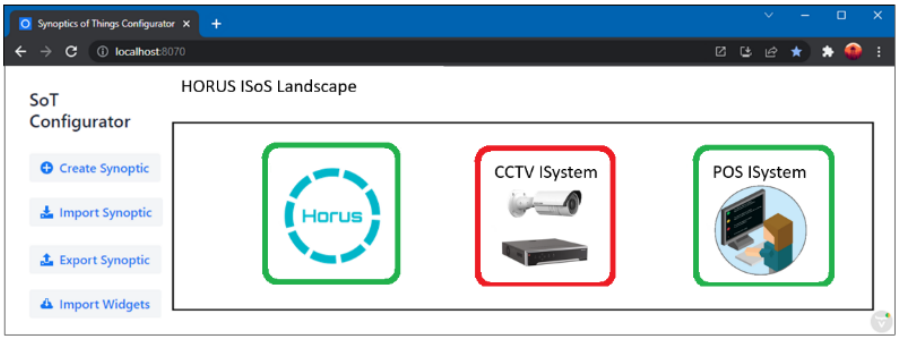

Fig. 3 – Synoptic of Things for a gas station forecourt that is using the HORUS project

Building the dashboard presented in **Fig. 3** is a quite straightforward procedure: i) Access the ISoS framework of the Organization through the well-known access point at the default port 2058; ii) Issue a lookup request to find the metadata of the existing

monitoring systems; iii) For each monitoring system, display the corresponding icon and a colored frame denoting the state of the system, for example, green, yellow, and red, respectively, corresponding to the states OK, Warning, or Problem. For example, using this syntax, the analysis of **Fig. 3** reveals that the HORUS and POS systems are operational, but there is a problem with the CCTV system. Then, by inspecting the metadata associated with the CCTV system and the corresponding monitoring system, denoted as "CCTC-M" in **Fig. 2**, it is possible to access a second-level synoptic for the elements that compose the CCTV system**.** From the analysis of this second synoptic, presented in **Fig. 4,** and once more using the same syntax for the color of the frames, we can see a problem with a particular camera. In this case, the camera with the label "AXIS P137" is the problematic element. Once resolved the problem, the states of the camera and the system CCTV will become OK.

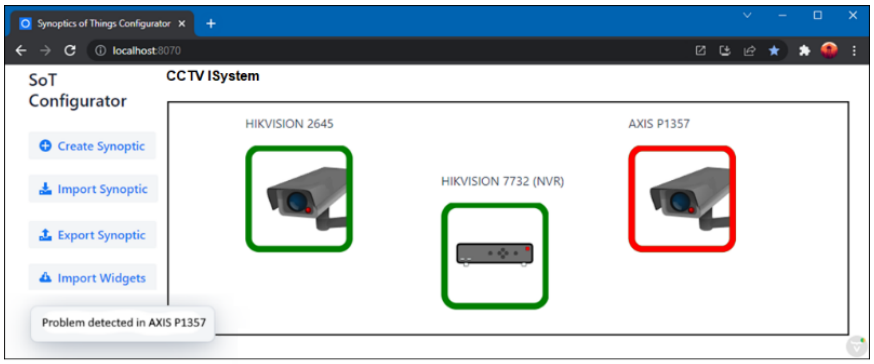

Fig. 4 – Synoptic for the CCTV system

Internally, each monitoring system on our research uses OpenNMS to collect data from the elements under monitoring using the SNMP protocol. The SoT framework uses the OpenNMS API to obtain the status of the service elements under monitoring. Also, using the OpenNMS API it is possible to send notifications to the users. For example, send an email to a system administrator when the state of a given element is critical. Another advantage of using the OpenNMS API, or the API of another monitoring system, is that a synoptic does not need to understand the protocols of the different elements under monitoring. It just needs to understand the API of the various monitoring systems. This approach makes possible a distributed monitoring, collaborative and scalable from the point of view of an organization. It can be further extended to monitor the state of elements in different organizations using a single synoptic if all the organizations adopt the ISoS framework (i.e., are ISoS enabled).

4. Conclusions and Further Research

This paper discusses the collaborative monitoring of informatics systems supported by the ISoS framework, which models an open organization's integrated computing technology landscape. The Java ecosystem adopting the Apache Zookeeper and other

open-source projects supports validating the ISoS framework, and the approach followed in the HORUS project. Beyond the $\texttt{ISystem}_0$ as a core technological element for any ISoS enabled organizations, we present and discuss the usage of the metadata stored within the ISoS framework to make possible the cooperation between monitoring systems that may exist within the informatics landscape of organizations participating in a collaborative network.

We further discuss the feasibility and advantages of using the ISoS metadata to feed a Synoptic of Things, extending the traditional concept of industrial synoptics of SCADA systems to show the status of the elements that exist in an organization's informatics technology landscape.

Although the case study presented in this work focused on the elements that exist in a forecourt gas station network of a single petroleum company, the case involves multiple supplying companies, each with interdependent responsibilities concerning their supported systems. Thus, it is reasonable to assume that the presented research results apply to scenarios involving networked organizations with interdependent responsibilities as long as they adopt the ISoS framework.

Acknowledgments. The research conducted by GIATSI/ISEL/IPL develops in collaboration with the SOCOLNET scientific network and its ARCON-ACM initiative. The ANSR/SINCRO, BP/HORUS, and FORDESI/SITL-IoT-PT-2020 projects partially support the research. Partial support also from the Center of Technology and Systems – UNINOVA, the Portuguese FCT Foundation (project UIDB/00066/2020). We also recognize the excellent contributions from Bruno Serras as a research fellow.

References

1. W. Barth. *Nagios: System and Network Monitoring*. No Starch Press, USA, 2nd edition, 2008. ISBN 1593271794.
2. F. Crespi, S. Caravella, M. Menghini, and C. Salvatori. European technological sovereignty: An emerging framework for policy strategy. *Intereconomics*, 56 (6): 348–354, nov 2021. doi: 10.1007/s10272-021-1013-6.
3. B. Farrell. *Web Components in Action*. Manning Publications, 2019. ISBN 9781617295775.
4. L. Furman and K. Zufelde. Network management : Open source solutions to proprietary problems. 2000. https://www.semanticscholar.org/paper/Network-Management-%3A-Open-Source-Solutions-to-Furman-Zufelde/7c9f70e43dfbf4f829a5ad96fec7108172e6b98d
5. C. Gonçalves, A. L. Osório, L. M. Camarinha-Matos, T. Dias, and J. Tavares. A Collaborative Cyber-Physical Microservices Platform – the SITL-IoT Case. In L. M. Camarinha-Matos, X. Boucher, and H. Afsarmanesh, editors, *Smart and Sustainable Collaborative Networks 4.0*, pages 411–420, Cham, 2021. Springer Int. Publishing. ISBN 978-3-030-85969-5. doi: 10.1007/978-3-030-85969-5_38.
6. M. Hause et al. The SysML modelling language. In *Fifteenth European Systems Engineering Conference*, volume 9, pages 1–12, 2006.

7. P. Hunt, M. Konar, F. P. Junqueira, and B. Reed. ZooKeeper: Wait-Free Coordination for Internet-Scale Systems. In *Proceedings of the 2010 USENIX Conference on USENIX Annual Technical Conference*. USENIX Association, 2010.
8. A. Kaushik. Use of Open Source Technologies for Enterprise Server Monitoring using SNMP. *Intl. Journal on Computer Science and Engineering*, 2, 10 2010.
9. L. Macura, J. Rozhon, and J. C.-W. Lin. Employing Monitoring System to Analyze Incidents in Computer Network. In J. Gottvald and P. Praus, editors, *Proceedings of the 3rd Czech-China Scientific Conference 2017*, chapter 7. IntechOpen, Rijeka, 2017. doi: 10.5772/intechopen.71102.
10. H. Maulana and Al-Khowarizmi. Analyze and designing low-cost network monitoring system using icinga and raspberry pi. *IOP Conference Series: Earth and Environmental Science*, 704 (1): 012038, mar 2021. doi: 10.1088/1755-1315/704/1/012038.
11. A. L. Osório, A. Belloum, H. Afsarmanesh, and L. M. Camarinha-Matos. Agnostic Informatics System of Systems: The Open ISoS Services Framework. In L. M. Camarinha-Matos, H. Afsarmanesh, and R. Fornasiero, editors, *Collaboration in a Data-Rich World*, pages 407–420. Springer Int. Publishing, 2017. ISBN 978-3-319-65151-4. doi: 10.1007/978-3-319-65151-4_37.
12. A. L. Osório, L. M. Camarinha-Matos, H. Afsarmanesh, and A. Belloum. Liability in Collaborative Maintenance of Critical System of Systems. In L. M. Camarinha-Matos, H. Afsarmanesh, and Á. O. Bas, editors, *Boosting Collaborative Networks 4.0 - 21st IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2020, Valencia, Spain, November 23-25, 2020, Proceedings*, volume 598 of *IFIP Advances in Information and Communication Technology*, pages 191–202. Springer Int. Publishing, 2020. doi: 10.1007/978-3-030-62412-5_16.
13. A. L. F. G. Osório. *Collaborative networks as open Informatics System of Systems (ISoS)*. PhD thesis, University of Amsterdam - Faculty of Science - Informatics Institute, Dec. 2020. URL https://hdl.handle.net/11245.1/233a4628-282e-4650-9ffb-b3d7b3187e2a.
14. T. Senst, M. Patzold, R. H. Evangelio, V. Eiselein, I. Keller, and T. Sikora. On building decentralized wide-area surveillance networks based on ONVIF. In *2011 8th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. IEEE, aug 2011. doi: 10.1109/avss.2011.6027365.
15. B. Serras, C. Gonçalves, T. Dias, and A. L. Osório. Synoptics of Things (SoT): An Open Framework for the Supervision of IoT Devices. In *5th International Young Engineers Forum on Electrical and Computer Engineering*. IEEE Xplore digital library, 2021. doi: 10.1109/YEF-ECE52297.2021.9505145.
16. B. Serras, C. Gonçalves, T. Dias, and A. L. Osório. Extending the Synoptics of Things (SoT) Framework to Manage ISoS Technology Landscapes. In *To appear in 6th International Young Engineers Forum on Electrical and Computer Engineering*. IEEE Xplore digital library, 2022.
17. K. Shiotsuka. Combining ot, it, and products to help realize society 5.0, May 2022. URL https://www.hitachi.com/rev/archive/2018/r2018_05/message/index.html.
18. N. Sukhija and E. Bautista. Towards a framework for monitoring and analyzing high performance computing environments using kubernetes and prometheus. In *2019 IEEE SmartWorld, Ubiquitous Intelligence &amp Computing, Advanced &amp Trusted Computing, Scalable Computing &amp Communications, Cloud &amp Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, aug 2019. doi: 10.1109/smartworld-uic-atc-scalcom-iop-sci.2019.00087.
19. R. I. E. Villalobos, E. A. Triana, H. Z. Ceballos, and J. E. O. Triviño. Design and Implementation of Network Monitoring System for Campus Infrastructure Using Software Agents. *Ingeniería e Investigación*, 42 (1): e87564, jul 2021. doi: 10.15446/ing.investig.v42n1.87564.