Liability in Collaborative Maintenance of Critical System of Systems

A. Luis Osório, Luis M. Camarinha-Matos, Hamideh Afsarmanesh, Adam Belloum

Liability in Collaborative Maintenance of Critical System of Systems

A. Luis Osório[1], Luis M. Camarinha-Matos [2], Hamideh Afsarmanesh[3], Adam Belloum[3]

[1]ISEL - Instituto Superior de Engenharia de Lisboa, Instituto Politécnico de Lisboa, and POLITEC&ID, Portugal, lo@isel.ipl.pt
[2] Faculty of Sciences and Technology, NOVA University of Lisbon and CTS-UNINOVA, Portugal, cam@uninova.pt
[3]University of Amsterdam (UvA), The Netherlands {a.belloum, h.afsarmanesh}@uva.nl

Abstract. Our society is facing a growing dependency on services supported by multiple interconnected computing and cyberphysical artifacts, constituting complex systems-of-systems. Such dependence means that a web of technology suppliers and IT departments have the responsibility to guarantee the operational quality of such systems. In this scenario where dependable services are maintained and evolved by networks of organizations, the question is how to ensure a liability framework able to reduce or help to solve potential legal conflicts. This work on liability in Collaborative Maintenance of Critical System of Systems grounds on previous research on the open Informatics system of systems (ISoS) framework. It extends the ECoNet collaborative network infrastructure with facets to support liability and maintenance. We propose and discuss a strategy for the management of evidence towards a conflictless collaborative context for the maintenance of critical systems-of-systems.

Keywords: Complex Informatics System of Systems, Distributed Systems, Collaborative Networks, Dependability

1 Introduction

Achieving reliable complex digital environments requires the management of collaborative maintenance among providers of computing and communication technology artifacts. The fact that complex digital technology systems (system-of-systems) are of the responsibility of different stakeholders, and in some cases, share technology elements, the origin of failures is hard to identify. The proper operation of such systems requires stakeholders to collaborate in the diagnosis and maintenance interventions. The understanding of interdependencies and the complex interconnections of a network of systems manifested through shared states are, according to [10], essential to evaluate associated operational risks.

For instance, a helpdesk ticket service integrating fault ticket events from a diversity of sources, either from systems and manual origin, which decides about responses to repair situations, is an example of a complex system of systems. However, the traditional organization of software products lacks preparation from inception for

collaborative multi-stakeholder support and maintenance. In many cases, accountability models and intervention plans, answering failure events under automated procedures, are not available. The maintenance of shared products/components requires stakeholders to coordinate maintenance services under complex liability contracts. Collaborative maintenance also needs to be supported by proper interactions among informatics systems from various application domains, e.g., accounting, billing, operational teams scheduling, and negotiation. At a higher abstraction level, business processes need to manage such collaborative liability in a streamlined and efficient way.

Collaborative maintenance of complex systems needs, therefore, the formalization of "responsibility borders" and specific liability-oriented interactions among technology systems, which are currently not adequately addressed by existing products. Despite numerous research contributions to structure computing and communication artifacts, existing products commonly establish isolated islands without formal mechanisms to model dependencies among elements of different suppliers. An adequate liability framework would require a standardization of technology artifacts, data and process models, and interactions between system elements. Towards this aim, in [4], a system concept is proposed as an entity that interacts with others establishing a system boundary. However, a formal model to support the management of such computing entities is still lacking.

This research further discusses an approach for dependability based on previous research on error detection, fault diagnosis, and recovery [3] that seems a crucial contribution to our study. Our paper extends these ideas and our previous research work on formal models for both a collaborative enabled and liability framework, namely by structuring the organization's computing and cyberphysical artifacts based on the ISoS framework [15], [14]. We also consider related research on computing services, guided by the HORUS industry problem [6], to propose a strategy based on the Collaborative Network concepts.

2 Guiding Use Case

In this paper, we analyze the HORUS case study where multiple stakeholders are responsible for subsets of technology artifacts in a forecourt (fueling station). The main problem, in this case, is the lack of systemic model structuring computing and cyberphysical elements and the formalization of a collaboration-enabled framework for technology artifacts and liability framework. Our approach to the HORUS system maintenance considers three cooperating informatics systems: (1) The HORUS core system, responsible for post-payment control, (2) the point of sale (POS) managing payments, and (3) the CCTV, managing the video cameras and video recorders. As such, the technology systems in this fueling station depend on computing and cyberphysical elements under the responsibility of three stakeholders, respectively, company A (payment enforcement system), company B (fueling payment system), and company C (security and surveillance systems).

The HORUS system is responsible for the payment enforcement, meaning validating a vehicle that requests fueling to be authorized by the Point-of-Sails (POS) system.

When a vehicle stops at a fuel station close to a pump, the HORUS system collects its license plate through a License Plate Recognition (LPR) component and the respective video camera. When the POS system (of the responsibility of company B) receives a fueling request from a pump, it asks the HORUS core system (of the responsibility of company A) if the customer has any pending payment. The LPR component, which used to identify vehicles, depends on video cameras that are managed by the CCTV system (of the responsibility of company C).

When a problem exists with a camera, e.g., it tilts down, the operator at the POS console detects a yellow icon, meaning that the HORUS core system did not answer the pending payment validation. In a situation like this, it is common to call all stakeholders to contribute to resolving the problem. Empirical evidence shows that, in most cases, the resolution of the issue would only need a CCTV technician from company C. Furthermore, to guarantee that a POS operator always sees a green or red icon is not trivial. A green icon means the vehicle has no pending payments, while a red one means that a no-payment event exists. When the screen icon is red, the standard procedure is to call the customer to resolve the case before authorizing the vehicle can get fuel. The minimization of occurrences of yellow icons resulting from some failure needs a novel collaborative liability and governance model to improve monitoring and maintenance interventions. The challenge is to restrict requests to those who need to intervene to fix some technology part under their responsibility.

Grounded on previous research on developing an open informatics system of systems (ISoS), the concepts of informatics system (Isystem) and Cooperation Enabled Services (CES), and the Collaborative network infrastructure ECoNet) [17] are now explored and extended to address liability challenge related to the proper operation of technological artifacts.

3 Research Trends and Industry Approaches

The area of systems' maintenance has a long tradition in addressing how to guarantee that manufactured systems work correctly. For instance, in [19], a definition of maintenance is presented as a "*set of activities required to keep physical assets in the desired operating condition or to restore them to this condition*." We suggest updating the definition by considering a maintenance system like the one guaranteeing that a set of technological artifacts work correctly under the quality of services contract. The difference is in the subject of maintenance.

The need to consider increasing integration requirements establishes a complex web of the interrelated technology artifacts. The growing adoption of smart things in the sense that technology systems more and more incorporate some physical elements with embedded computing and communication capabilities suggests a novel approach to integration. Since technology artifacts are connected things, commonly referred to as Cyber-Physical Systems (CPS) / Internet of things (IoT), they can incorporate a monitoring view by implementing instrumentation services to plug a monitoring infrastructure [5]. Taking our fueling forecourt case and considering that gate locking elements tend to be electronic and somehow integrated, it makes it possible to infer about its proper functioning. Such technology artifacts require monitoring, and there is,

therefore, a need to frame them into some novel monitoring framework. The assumption in [19] oriented to technology as physical assets, needs a new abstraction layer to model technology assets as elements of a system composed of independent computational elements. By independent computational elements, we mean artifacts with computing and communication capabilities. Our interest is for independent (smart) elements meaning that our understanding of monitoring refers to technology artifacts led by a computational decision center.

In [19], an overview of the timeline of the maintenance function mentions cooperation. In this timeline, a "cooperative partnership" perspective occurs around 2000. The cooperative and collaborative aspects are explored further in [9] as key aspects of monitoring. In the context of the TEMIC project, the mentioned authors present and discuss a platform to remotely or locally integrate autonomous supervision, monitoring, and maintenance management systems by emphasizing the collaboration perspective.

More recent research confirms the trend towards a collaborative view as technology artifacts are more connected and application domains interleaved, requiring higher integration degrees. The MANTIS project is an example aiming at developing a "*proactive maintenance service platform architecture based on Cyber-Physical Systems*" [13]. In the context of the same project, in [18], the concept of Collaborative Maintenance is motivated by the "*optimum maintenance of assets, different systems, and stakeholders have to share information, resources, and responsibilities, i.e., collaboration is required*."

Collaborative maintenance is also a research topic associated with industry 4.0 [7]. For instance, the research reported in [21] proposes a strategy and a system for the monitoring of a car engine production line aiming at reducing breakdowns of shop-floor machines that typically prevent the lines from operating for hours. As such, the authors proposed a collaborative maintenance strategy through a context-aware system that makes operators aware of the problems. However, in this and other research works, formulated questions are centered on integration without a particular emphasis on responsibility or liability issues. For instance, the research in [21] is, in fact, more concerned with stoppage time and the impact on the production line. No research work, to our knowledge, addresses liability by discussing interdependencies among systems, considering subsets of elements (or systems), under different responsibilities, e.g., maintained by different supplying companies.

4 Adopting the ISoS Systems Modularity Framework

The lack of a well-founded model for the coordination of the participating stakeholders in collaborative maintenance of a critical system of systems (SoS) motivates our research towards a strategy for liability management.

The recent trend to "see" a web of things accessed by the integration of services running on the cloud does not seems to match practical coordination models delimited by restricted contexts (system's responsibility). We can consider a video camera in a fueling forecourt accessed as a thing in the context of some cloud level service (IoT application) [2]. However, a video camera is a thing that is part of some system, the

abstraction responsible for its lifecycle management. In the HORUS case, the HORUS informatics system shares access to cameras to identify vehicles positioned for fuelling. However, the camera is of the responsibility of the abstraction that manages the life cycle of video surveillance-related elements, e.g., video cameras, video server recorder, from other subsystems. **Fig. 1** depicts a simplified view of this scenario, showing three informatics systems (Isystems) that cooperate with the HORUS Isystem.

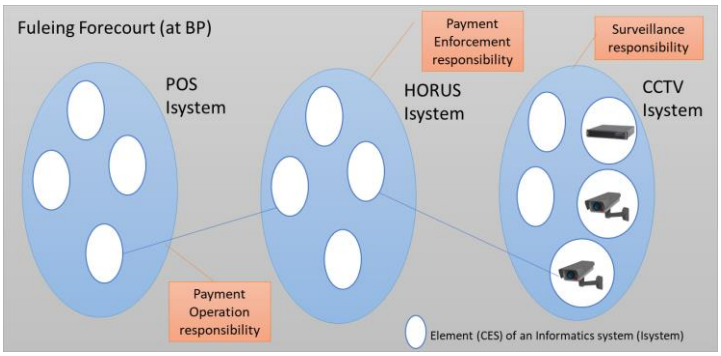

Fig. 1. The primary computational and cyberphysical responsibilities in a forecourt

The adoption of a framework like ISoS by the industry is a complicated, slow, and risky process. In our work, the support of BP Portugal, expressed by the willingness to evolve to a competitive multi-supplier scenario, has been of paramount importance. Being HORUS, an Isystem of our responsibility and the start-up Exploitsys responsible for its support and maintenance, we can influence the validation and adoption of new models. The adoption of ISoS is, however, constrained since it requires changes in the deployed critical system (legacy artifacts). Given the involved costs and operational risks, companies are as conservative as possible. The current implementation of the HORUS Isystem is already monitored by a system that collects (instruments) behavior data from the system's components to infer about their proper functioning. The Exploitsys company adopted the OpenNMS, an open-source system based on the Java technology ecosystem and OSGi specifications and implementations for this purpose. The OpenNMS[1] monitoring system is a paradigmatic example of a product grounded on a project developed under the open-source model since its formation in 2002 [1] and widely adopted by industry and by the research community.

In the following sections, we detail our research strategy to evolve from the current implementation to a collaborative model where monitoring of each informatics system has its monitoring strategy. Such a monitoring process has the additional responsibility to manage functional relationships between elements of different informatics systems prone to generate liability conflicts in establishing which of the system assumes the consequences of failure.

[1] https://www.opennms.com/

4.1 The Proposed Approach for a Collaborative Monitoring

The proposed strategy is to adopt the ISoS modularity framework as a basis. Instead of taking a monolithic architecture as followed by other works, we intend to preserve the business responsibilities and map them to the Informatics System (Isystem) concept. It means that a hierarchical monitoring framework considering (intra) Isystems decisions replaces the current flat interconnection between elements under different business responsibilities.

While initially validating for the video cameras case, the model considers each Isystem (POS, HORUS, and CCTV) has a corresponding tandem Isystem responsible for monitoring the proper operation of the related informatics system (respectively, POS-M, HORUS-M, CCTV-M). In the particular case of the HORUS Monitoring (HORUS-M) Isystem, the video camera is the type of element selected to validate the proposed approach, as depicted in Fig. 2. The collaborative monitoring involves an additional informatics system class responsible for coordinating the specialized informatics systems, which we designate by Integrated Monitoring (Integrated-M).

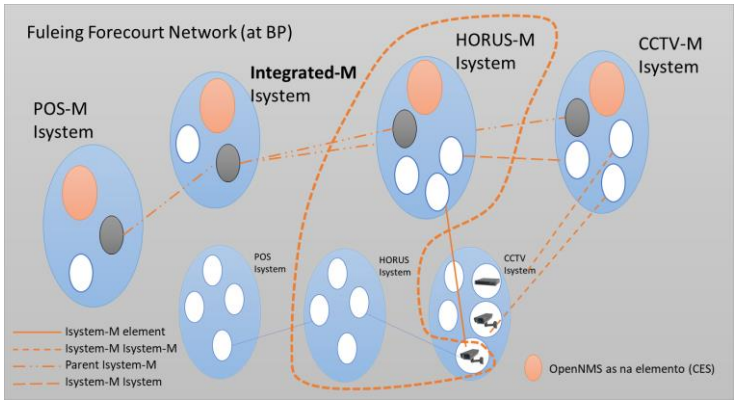

Fig. 2. Proposal of a hierarchical collaborative monitoring context

The region delimited by a dashed line represents the as-is that needs to evolve to the proposed model. Meanwhile, the HORUS-M Isystem directly accesses the video cameras. We expect from Prosegur (a surveillance company) the adherence to the ISoS model to change their management systems to cope with the purposed approach. The plan is to validate the HORUS-M concepts accessing directly through a specific (adapter) element to connect directly to the video cameras using ONVIF[2] protocols. This adapter will evolve later for the service concept in the ISoS model with the adoption of the CCTV-M Isystem.

The apparent throwing out (eventually seen as a demotion) of the OpenNMS informatics system as an element of the suggested Isystem-M might be at first confusing. The idea is to frame the valuable computational responsibilities already offered by OpenNMS into a broader and integrating framework, making explicit the different responsibilities at the organization technology landscape level. Current

[2] https://www.onvif.org/

approaches do not follow formal delimitations of technology artifacts, leading to conflicts when making some suppliers accountable for failures with business costs consequences. Furthermore, our option for OpenNMS considered its open development model and the fact that it grounds on Java/OSGi with an emphasis on the open specifications. While the ISoS deals with technology diversity, the development costs, and the willingness to reduce vendor dependencies suggests a technology convergence strategy to minimize heterogeneity.

Another not trivial aspect is the fact that OpenNMS, by conception, addresses the monitoring of network-level elements primarily. The Simple Network Management Protocol (SNMP) and related concepts like the Management Information Base (MIB) modeling data properties with associated Object Identifiers (OIDs) underly the OpenNMS monitoring system. Any instrumentation variable, e.g., in a trap or other message, has an associated OID [23].

4.2 The Need for Collaborative Monitoring

Although from the conceptual viewpoint, the proposed strategy has a straightforward appearance, when considering legacy systems and elements to evolve, it requires investment and changes in related legacy or new technology systems and processes. As an example, when a problem in a video camera occurs, the HORUS-M receives a trap event, the camera agent triggers (SNMP terminology). However, since the HORUS system supported by Exploitsys is using a camera device of the responsibility of another supplier, in our case, Prosegur, the question is: why not to forward the event directly to the "owner" of the technology element? It is technically possible, however since both companies compete for the best service for the BP Portugal company, why should Exploitsys assume the responsibility to forward trap events? Or should the trap events be managed and sent by an independent coordination system, i.e., collaborative monitoring coordination operationalized by Integration-M, as depicted in **Fig. 2**?

The HORUS collaborative monitoring case is simple since it does not involve a massive number of technological artifacts. However, at the same time, it is complex enough to validate alternative collaborative monitoring coordination models since it includes at least three independent suppliers. One main challenge here is to establish a collaboration model able to join at some unique decision coordination point the support interventions after a careful and reliable diagnosis process.

In a different application domain (healthcare), the design of an electrocardiogram (ECG) monitoring systems, as presented and discussed in [20], is an example of an integrated monitoring system in a critical application domain. The proposed architecture follows the integration of a diversity of technology artifacts from sensors to computational decision support entities where some are executed on the cloud with the primary concern to guarantee the quality of services considering enforcement, security, and smartness. The introduced smartness is to provide "*flexibility and enable interoperability between a myriad of healthcare monitoring devices*.". The approach, however, shows a monolithic architecture that seems complicated to plug as a subsystem into a broader healthcare collaborative monitoring environment. Each technology artifact being either a cyberphysical element (sensor/actuator) or a pure

computational part running somewhere on a computational platform (on-premises, cloud, for), needs to be under an integrated monitoring strategy.

In our ISoS approach [16], each computational responsibility structures as services organized as compositions establishing CES as an element of an informatics system. The informatics system (Isystem) concept determines the computational responsibility commonly attributed to the supplier, the responsible of the Isystem support. Under our ISoS framework, we would consider the Electrocardiogram Informatics System, the ECG Isystem, and an ECG-M, ECG Monitoring Informatics System, as a different system responsible for monitoring the ECG elements, both computational and cyberphysical [20].

Monitoring is of paramount importance to delimit and accurately assign liabilities from the occurrence of any failure. A complex system of systems with system elements shared among different Isystems establishes aggregations that are challenging to maintain and evolve. When a component fails, as possible, the problem shall be detected, diagnosed, and repaired by supporting responsibility at the coordination abstraction layer. In our approach to avoid disturbing Exploitsys (responsible for HORUS Isystem), we proposed that when a video camera in a fueling forecourt fails for some reason, it is of the responsibility of CCTV-M to signal HORUS-M that the problem is under resolution. Furthermore, before the HORUS Isystem detects a problem in a video camera, we expect that the technician from Prosegur is in the process of repairing it. Our proposed separation of concerns, namely: i) operation with the responsibility of the Isystems HORUS and ii) monitoring with the responsibility of the Isystems CCTV, and the accountability of the tandems, HORUS-M and CCTV-M, aims to facilitate the development of intelligent collaborative strategies to diagnose and identify recurrent problems and suggest changes.

5 Liability Managed at Collaborative Networked Level

The experience with the HORUS deployment has been raising new questions, namely the need for some new form of coordination among suppliers of both technology artifacts and services. As prevalent in large organizations, a helpdesk service provider centralizes and coordinates repairing tickets from a diversity of origins, from manual ones to automatically generated in legacy applications (Isystems in our terminology). The emails continue being the preferred support for ticket information exchange, making it challenging to integrate approaches where automatic events integrate partner's maintenance business processes. One important aspect is to establish a governance model for such collaborative maintenance cases. A key research question is how to preserve the liability of each supplier since the proper functioning of business activities depends on intertwined cooperation relationships among technology systems under different support responsibilities.

Based on the ECoNet research [17], we propose that the second monitoring coordination layer, our Integration-M, takes the responsibility of cooperating with a Helpdesk Isystem that coordinates tickets and maintenance operations through the services of the ECoNet platform as depicted in **Fig. 3**.

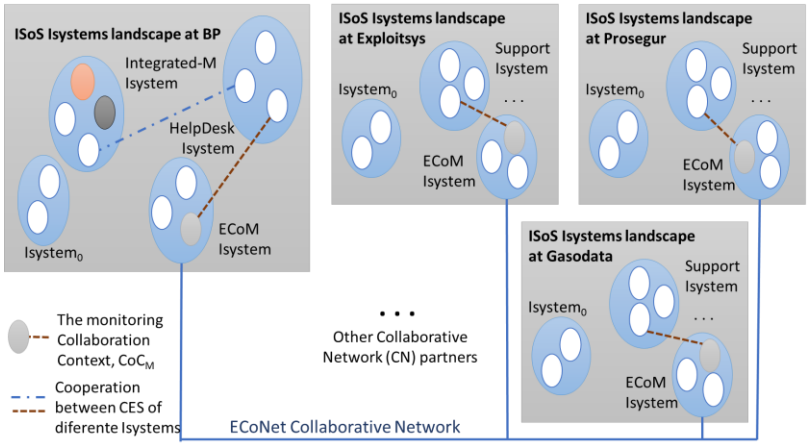

Fig. 3. Adopting ECoNet CN platform to coordinate collaborative maintenance

The legacy adapters implementing the exchange of data or control between organizations evolve to adopt the unified Collaborative Context (CoC). In our collaborative monitoring, the strategy is to persuade companies to utilize the open ECoM Isystem. As already discussed, this requires a change to the current approach, where technology artifacts depend on specific architectures. With our approach, by structuring computational responsibilities under the proposed ISoS framework [15], would facilitate technology landscapes with well-defined "responsibility borders", and in this way, enable evolution towards agnostic technology landscapes. However, the problem is much more complicated than the technology diversity. Since a network of stakeholders is involved, where each company has its technology and processes culture, there is a need for a coordination strategy able to minimize interoperability risks. Coordination is a crucial concept for understanding liability and dependability, and it remains recurrent research for decades.

About two decades ago [12] suggested coordination from three perspectives: i) impacts of information technology on persons and markets, ii) design of cooperation tools, and iii) design of distributed and parallel computer systems. Twenty years later, the approach to coordination needs updated terminology and concepts, but the core problem remains. Mapping the proposed perspective to our strategy implies: i) the need to design Isystems answering organization, workers, and market needs, ii) to consider Isystems as automation computing artifacts or implementing functionalities for users (tools) need to answer collaboration needs, and iii) the underlying execution environments on-premises or on the cloud need to be reliable, elastic, secure, in supporting system of Isystems at each networked organization. However, the diversity of legacy models and approaches to systems make challenging the endeavor to design collaborative maintenance to manage the liability properly.

The assumption from our industrial partner of the long-term characteristics of the changes has been of paramount importance. Since suppliers naturally compete for being the only one offering a product or a service, the changes for the necessary preparedness to join a collaborative network needs a third force – the user organization. The Porter's

diamond discussed in the context of competition in the software industry [22] slightly updated by changing software by Isystems and changing "Related and Supporting Industries" by user-organizations shows a similar pattern to our proposed strategy. The renewed challenge is how should the holistic solutions cope with market competition to avoid the current vendor-lock-in situation. We argue that by applying our approach of developing an agnostic ISoS framework [15], we achieve added quality and competing costs. There is, however, the need for changing the discourse from software to Isystems, the proposed "systems thinking," leading to integrated collaborative monitoring for the system of systems in a collaborative network context. More than a decade later [11] Porter's diamond is decorated by the *Chance* and *Government* concepts as additional dimensions interpreted as facilitators for competition. The *Government* dimension confirms the need for investment in research and validation through pilots. Public or user organization investment, on the one hand, helps to "impose" the move from the vendor-specific through open standards to the systems thinking where solutions evolve towards agnostic decisions at procurement processes. On the other hand, as a strategy to induce market competition and get products and services at sustainable costs [15].

In our approach, the adoption of the ISoS framework structuring and enhancing the technology infrastructure with four monitoring informatics systems aims to establish an accountability border formed by the respective operational and tandem monitoring Isystems. Each tandem monitoring Isystem has the responsibility of detecting any element malfunction of the respective Isystem. It means that when a video camera shows some king of breakdown, e.g., for some reason, the resolution changed, a trap is generated by the camera's monitoring agent (SNMP agent) to be managed by the CCTV-M Isystem. The CCTV-M Isystem notifies the Integrated-M, that forwards the occurrence to the monitoring tandem of Isystems that depends on the camera of the responsibility of CCTV Isystem, in our case, the HORUS-M. Since the exchange of data to supplier's support Isystems managed by the Helpdesk Isystem in coordination with Integrated-M as depicted in **Fig. 3**, any delay in repairing the camera is of the responsibility of the CCTV Isystem supplier. Depending on specialized collaborative monitoring processes, the suppliers with interdependent elements are this way able to follow-up mutual maintenance interventions and being aware of potentially related failures in the Isystem(s) they are responsible for supporting.

5 Conclusions and Further Research

This paper presents and discusses ongoing research on liability in Collaborative Maintenance of the Critical System of Systems. The open Informatics system of systems (ISoS) framework and the ECoNet collaborative network infrastructure is adopted to structure a collaborative monitoring strategy for a petroleum distribution company. The approach aims to formalize accountability borders for suppliers of informatics and cyberphysical systems, with share elements. The approach considers that each operational Isystem has a tandem monitoring Isystem responsible for monitoring its proper operation. The model applies to a fueling distribution network

and plans to involve three main Isystems (POS, POS-M, HORUS, HORUS-M, and CCTV, CCTV-M) that interact in the context of the fueling management process.

Beyond the need to evolve strategies and models to conciliate de legacy systems and development initiatives as the case of the OpenNMS open-source project, higher-level abstractions need to be designed and validated. An interesting example is to establish liability models to be managed and decided at the Integrated-M level quality of service rates according to the experienced behavior of each Isystem and taking into account interdependencies and proper actions concerning each supplier responsible for the support (maintenance). The liability of suppliers accountable for complex interdependent Isystems and its mapping to an appropriate and fair management of quality of services of each responsibility needs further research.

Acknowledgments. The research conducted by GIATSI/ISEL/IPL develops in collaboration with the SOCOLNET scientific network and its ARCON-ACM initiative. BP Portugal, through the research project HORUS, A-to-Be (Brisa Innovation and Technology) with the research MOBICS/CITS, and FORDESI SITL-IoT through the PT-2020 research project, partially supports the research work. The participation of the start-ups Exploitsys and Makewise has been of paramount importance. Partial support also from the Center of Technology and Systems – UNINOVA, and the Portuguese FCT Foundation (project UIDB/00066/2020), and the European Commission (project DiGiFoF).

References

1. M. Andreolini, M. Colajanni, and M. Pietri. A scalable architecture for real-time monitoring of large information systems. In *2012 Second Symposium on Network Cloud Computing and Applications*, pages 143–150, Dec 2012.
2. Hany F. Atlam, Robert J. Walters, and Gary B. Wills. Fog computing and the internet of things: A review. *Big Data and Cognitive Computing*, 2(2), 2018.
3. Algirdas Avižienis. Design of Fault-Tolerant Computers. In *Proceedings of November 14-16, 1967, Fall Joint Computer Conference*, AFIPS '67 (Fall), page 733-743, New York, NY, USA, 1967. Association for Computing Machinery.
4. Algirdas Avižienis, Jean-Claude Laprie, and Brian Randell. Dependability and Its Threats: A Taxonomy. In Renè Jacquart, editor, *Building the Information Society*, pages 91–120, Boston, MA, 2004. Springer US.
5. Joao M. F. Calado and A. Luis Osorio. *Dynamic Integration of Mould Industry Analytics and Design Forecastings*, pages 649–657. Springer International Publishing, Cham, 2017.
6. L. M. Camarinha-Matos, H. Afsarmanesh, E. Ermilova, F. Ferrada, A. Klen, and T. Jarimo. ARCON reference models for collaborative networks. In: Luis M. Camarinha-Matos and Hamideh Afsarmanesh, editors, *Collaborative Networks: Reference Modeling*, pages 83–112. Springer US, 2008. 10.1007/978-0-387-79426-6_8.
7. Luis M. Camarinha-Matos, Rosanna Fornasiero, Javaneh Ramezani, and Filipa Ferrada. Collaborative networks: A pillar of digital transformation. *Applied Sciences*, 9(24), 2019.
8. P. Capodieci, S. Diblasi, E. Ciancamerla, M. Minichino, C. Foglietta, D. Lefevre, G. Oliva, S. Panzieri, R. Setola, S. D. Porcellinis, F. D. Priscoli, M. Castrucci, V. Suraci, L. Lev, Y. Shneck, D. Khadraoui, J. Aubert, S. Iassinovski, J. Jiang, P. Simoes,

F. Caldeira, A. Spronska, C. Harpes, and M. Aubigny. Improving resilience of interdependent critical infrastructures via an on-line alerting system. In *2010 Complexity in Engineering*, pages 88–90, Feb 2010.

9. E Garcia, H Guyennet, J.C Lapayre, and N Zerhouni. A new industrial cooperative tele-maintenance platform. *Computers & Industrial Engineering*, 46(4):851 – 864, 2004. Computers and Industrial EngineeringSpecial Issue on Selected papers form the 29th.International Conference on Computers and Industrial Engineering.
10. Yacov Y. Haimes. Risk modeling of interdependent complex systems of systems: Theory and practice. *Risk Analysis*, 38(1):84–98, 2018.
11. Richard Heeks. Using competitive advantage theory to analyze it sectors in developing countries: A software industry case analysis. *Information Technologies and International Development*, 3:5–34, 2007.
12. Thomas W. Malone and Kevin Crowston. The interdisciplinary study of coordination. *ACM Comput. Surv.*, 26(1):87â€“119, March 1994.
13. Urko Zurutuza Ortega. The mantis book. cyber physical system based proactive collaborative maintenance. 2019.
14. A. Osorio, Luis Camarinha-Matos, and Hamideh Afsarmanesh. Cooperation Enabled Systems for Collaborative Networks. In Luis Camarinha-Matos, Alexandra Pereira-Klen, and Hamideh Afsarmanesh, editors, *Adaptation and Value Creating Collaborative Networks*, volume 362 of *IFIP Advances in Information and Communication Technology*, pages 400–409. Springer Boston, 2011. 10.1007/978-3-642-23330-2_44.
15. A. Luis Osorio. *Towards Vendor-Agnostic IT-System of IT-Systems with the CEDE Platform*, pages 494–505. Springer International Publishing, Cham, 2016.
16. A. Luis Osorio, Luis Camarinha-Matos, Hamideh Afsarmanesh, and Adam Belloum. *Towards a Mobility Payment Service based on Collaborative Open Systems*. In: Collaborative Networks and Digital Transformation. PRO-VE 2019. IFIP Advances in Information and Communication Technology, vol 568. Springer, Cham. https://doi.org/10.1007/978-3-030-28464-0_33, 2019.
17. Luis A. Osorio, Luis M. Camarinha-Matos, and Hamideh Afsarmanesh. ECoNet Platform for Collaborative Logistics and Transport. In: *Risks and Resilience of Collaborative Networks*, volume 463 of *IFIP Advances in Information and Communication Technology*, pages 265–276. Springer International Publishing, 2015.
18. G. Papa, U. Zurutuza, and R. Uribeetxeberria. Cyber physical system based proactive collaborative maintenance. In *2016 International Conference on Smart Systems and Technologies (SST)*, pages 173–178, Oct 2016.
19. Liliane Pintelon and Alejandro Parodi-Herz. *Maintenance: An Evolutionary Perspective*, pages 21–48. Springer London, London, 2008.
20. Mohamed Adel Serhani, Hadeel T. El Kassabi, Heba Ismail, and Alramzana Nujum Navaz. Ecg monitoring systems: Review, architecture, processes, and key challenges. *Sensors*, 20(6), 2020.
21. Konstantinos Sipsas, Kosmas Alexopoulos, Vangelis Xanthakis, and George Chryssolouris. Collaborative maintenance in flow-line manufacturing environments: An industry 4.0 approach. *Procedia CIRP*, 55:236 – 241, 2016. 5th CIRP Global Web Conference - Research and Innovation for Future Production (CIRPe 2016).
22. M. St.Quintin. Competitive advantage in the software industry. *WIT Transactions on Information and Communication Technologies*, 1993.
23. Z. Wang, Y. Wang, and G. Shao. Research and design of network servers monitoring system based on snmp. In *2009 First International Workshop on Education Technology and Computer Science*, volume 3, pages 857–860, 2009.