SAND2018-11231C

Toward a Multi-Agent System Architecture for Insight & Cybersecurity in Cyber-Physical Networks

William M.S. Stout
Sandia National Laboratories
Albuquerque, New Mexico, USA

***Abstract*—Operational Technology (OT) networks existed well before the dawn of the Internet, and had enjoyed security through being air-gapped and isolated. However, the interconnectedness of the world has found its way into these OT networks, exposing their vulnerabilities for cyber attacks. As the global Internet continues to grow, it becomes more and more embedded with the physical world. The Internet of Things is one such example of how IT is blurring the cyber-physical boundaries. The eventuality will be a convergence of IT and OT. Until that day comes, cyber practitioners must still deal with the primitive security features of OT networks, maintain a foothold on enterprise and cloud networks, and attempt to instill sound security practices in burgeoning IoT networks. In this paper, we propose a new method to bring cyber security to OT and IoT-based networks, through Multi-agent Systems (MAS). MAS are flexible enough to integrate with fixed legacy networks, such as ICS, as well with be burned into newer devices and software, such as IoT and IT networks. In this paper, we discuss the features of MAS, the opportunities that exist to benefit cyber security, and a proposed architecture for a OT-based MAS.**

***Index Terms*—multi-agent system, IoT, OT, ICS, cyber security**

I. Introduction

Industrial Control Systems/Internet of Things/Operational Technology (I/OT) networks and their variants all share similarities in how their devices and networks bridge the cyber-physical domain. Not only is the primitive functionality shared, but also the lack of conventional cybersecurity techniques [1]. These systems are often accessed remotely by a variety of entities including utility workers, multiple third-party vendors, consumers, brokers, and other machines, where vetting and control of access may be cumbersome or impossible based on the equipment used. As a consequence, these Internet-connected devices that control and monitor physical processes are at risk of disruption by cyber-initiated attacks, and may provide additional paths through which attacks may be carried out [2]. Enterprise and cloud networks may enjoy the availability of resources to support cyber-hardening, -visibility, and -response; the constrained resources of I/OT networks do not readily accommodate upgrades, replacements or bolt-on solutions for cyber security. Furthermore, given the safety requirements of some systems, downtime to implement changes may not be acceptable. Thus, as adversaries have begun to recognize the minimal workfactor required to attack these networks, have cyber practitioners now begun to observe the effects from lackluster security. From smarthomes, to medical devices, to national powergrids, the attack space has seen [3] [4] [5]:

- Signal emulation (man-in-the-middle)
- Sensor influence/hijacking
- Eavesdropping
- Malware/Ransomware
- Denial-of-Service
- Device destruction

This problem-space is concerning and far-reaching. Historically, methods to secure I/OT networks have pointed to solutions that cannot be reasonably implemented due to legacy equipment, vendor complicity, or cost. A new approach is needed that can address these issues, but still be flexible to grow with new cybersecurity techniques and the advancement of network infrastructure. Corollary networks to I/OT are cloud and business networks, whose assets also operate in the open-Internet. A successful security paradigm in these networks is largely based on agents. The solution described herein borrows from this mindset and acts in the research space of Multi-Agent Systems (MAS).

In this paper, we start by covering the benefits and opportunities that exist to implement such a system (Sections II and III). In Section IV, we provide a brief overview of intelligent agents and multi-agents systems, followed by current research in the MAS space. Section V covers our description of the necessary attributes for an out-of-band Autonomous Agent (AA) network. We then conclude this paper in Section VI.

II. Benefits vs State-of-the-Art

Current state-of-the-art cybersecurity in I/OT is most prevalent with "big-box" vendors: username/passwords, embedded certificates, block-chain, etc. Often, these methods rely on:

1) Greenfield deployments.
2) Proprietary solutions.
3) Retrofitting.

The lot of these increase the stress on endpoints and disproportionately drive up costs (both monetarily and resource-wise) on low-performance, -compute, -bandwidth, and -energy

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

devices. We conjecture the solution does not lie in applying enterprise-like security - they are not the same (encrypted links do not prevent hijacking sensors). Response mechanisms for safety often do exist in I/OT networks, the crux lies in identifying maliciousness. Leveraging a Multi-agent System (MAS) attempts to usher in:

- intelligent, uninfluenced visibility,
- extensibility to other network-types,
- interfaces to support additional responses/defenses.

Literature does describe a particular relationship between MAS and I/OT networks; however, these solutions have encompassed the entire IoT system (e.g., its operation purpose) to decompose its components into agents of a MAS. This proposal significantly differs by decoupling the functionality of the two systems and establishing the MAS as a "watcher of the watchmen."

III. Opportunities

Critical infrastructure is a hot topic in the cyber security domain today. Given recent attacks with IoT [6], and attacks of the past [7], it's no wonder that governments are racing to refresh their operational technology networks. With so many advancements in the field of technology, now is an opportune time to augment, or even greenfield new deployments of these critical networks. Advances in networking through SDN have allowed the data center networks to ease configuration dynamically and push security down to the endpoint port through Network Function Virtualization (NFV). Computer virtualization and containerization have allowed endpoint security to flourish in new ways - ushering in new active defense techniques that waste time and resources of the adversary, but can also stifle attacks when needed.

There was a time when there was a strict divide between OT and IT; the OT networks were primarily based on availability at any cost. Once accreditation was passed and the network brought online, there was nothing that could be done to bring the network down - no patching, updates, reboots. The loss of network operations could result in a great loss of profits, or worse, could result in death. IT networks, on the other hand, were primarily based on information processing, sharing, and transfer. Here, the availability also mattered, but so did Confidentiality and Integrity of the data and network (the CIA principle). Installing patches, updating systems, making them more secure and more efficient were just as important as keeping them online.

However, within the past decade, have we see the cross-pollination of features between the two networks. The first sign of this was the advent of the Industrial Internet, where ICS processes and equipment were now getting connected though conventional Internet-based protocols (IP/TCP) to provide remote connectivity and access. And as devices in the home and field became "smarter" - greater amounts of centralized control was wanted (and needed) to ensure the devices operated as they should, and to gather information from them when needed. This led to the development of the Internet of Things, a new paradigm that bridged machine-based endpoints with the interconnected mesh of IT and the Internet.

The next forecasted shift on the horizon will be the complete melding of our business-based IT networks and those air gapped ICS networks [8]. It's happening now; SCADA network protocols are encapsulated in TCP and pushed across IT infrastructure. Businesses are beginning to realize that the networks *can* be supported by the same infrastructure, and are set to redesign OT and IT networks. New microgrid technologies are being stood up on campuses, leveraging SDN to provide "white-listed" flows across network segments. Vendors in the network and compute space are now designing equipment and software to support Software-Defined OT; not only is the network specified through a software-based controller, but the endpoints themselves are also virtualized, allowing the ease of defining physical processes through applications. This new paradigm has been branded the "Intelligent Edge," and is compatible with IT infrastructure [9] [10].

This software-based infrastructure brings with it new ways to draw in computational elements. The ability to process information at the edge, rather than have to bring it back to a central processing location, allows not only new ways to improve efficiency and congestion in network infrastructure, but also allows the ability to install software at the edge to detect, inform, and decide. Where physical security was paramount in ensuring ICS processes were carried out correctly, now with the shift in network technology, cyber security will be required to go all the way to the edge. Cyber attacks that once were reserved only for enterprises, will now be completely applicable to the the physical domain as well (the cyber-physical bridge).

IV. Multi-Agent Systems

Simply put, an agent is something that *acts* (Latin agere, "to do") [11]. With regard to computer science, all computer programs do something, but computer *agents* are expected to operate autonomously, perceive their environment, persist over a prolonged time period, adapt to change, and create and pursue goals. To say that an agent is *rational* is to say that it acts to achieve the best outcome or, through uncertainty, the best expected outcome.

Agents perceive their environments through *sensors* and act upon the environment through *actuators*. A *percept* is used to describe the agent's perceptual inputs at any given time; a *percept sequence* is the complete history of everything that agent has perceived. Thus, an agent's choice of action can be based on the entire percept sequence, but not on anything is has not yet perceived. And what the agent does (its behavior) is based on the agent function that maps percept sequence to an action.

A Multi-Agent System (MAS) is not unlike an organization, wherein the organization there exists several different departments charged to perform operations to meet the organization's goals. In the execution of those operations, each department may work independently of the others, but will often interact to exchange information when required. In the context of the

MAS, we can refer to those departments as agents. Each agent may constructed as singular or swarm entity, focused on a particular aspect supporting the MAS itself. That agent may be a physical entity (a sensor) or a software-based entity (a file scanner), whose capabilities require it to be:

1) Reactive: to be able to react to commands or changes in the environment
2) Proactive: to actively achieve its goals through interaction
3) Social: to communicate with other agents and perform as expected

These capabilities allow an agent to sense events in the environment, and actuate response as required. What brings an agent under the umbrella of AI is its ability to act autonomously, that is, to bridge the gap between sensing and actuating. This autonomy is relevant to the function of the agent, and may differ between agents. What an agent acts upon is defined by the agent's perspective, or the *Micro* Perspective. The collection of the agents' perspectives in the MAS go on to form the MAS perspective, or the *Macro* Perspective. The Macro Perspective is fed by the decentralized resources, knowledge and capabilities of the collective whole, providing a loose-coupling of the distributed agents. As a precursor to execution, agent-based modeling may be leveraged to ensure the system performs as expected given constraints, requirements, and the target environment. As an *organization*, the MAS is influenced and reacts through the autonomy of agents, learning as it continues to operate. The stability of the MAS is contingent on the requirement of coordination and cooperation between agents.

Coordination is needed between agents in to ensure the community of agents work together in a cohesive fashion [12]. Agents require coordination due to the fact that:

- agent goals may cause conflict internally or with agents,
- agents' goals may be interdependent,
- agents' may have different knowledges and capabilities,
- agents' goals may be accomplished faster if they work together.

Four approaches to aid with agent coordination include: (1) organizational structuring, (2) contracting, (3) multi-agent planning, and (4) negotiation. Organizational structuring relies on providing a hierarchical structure for the MAS, by defining roles, communication paths and authority relationships (e.g, client-server). In Contracting, agents may take on two roles, as either a manager or a contractor, where a manager decomposes a task into subtasks for which contractor agents makes bids for. Multi-agent planning, all of the agents in the MAS detail all future actions and interactions needed to achieve their goals, considering interdependencies that may require additional planning and re-planning. In this way, planning may be done through a central entity, or distributed. Finally, in Negotiation, all agents communicate with each other to reach an agreement on a matter or goal at hand. With such, the negotiation method can be either *competitive* or *cooperative*, based on the environment.

A. Literature Review

Multi-agent Systems have been a highly discussed research area for many decades. Early work can be found in the 1980s and 1990s, where MAS took the initial concepts of AI and made them more tangible [13]. As compute power has grown since then, MAS has been creeping back into the academic and research body, not unlike the way machine learning has, now that computer systems are armed with enough compute and memory resources to carry out not only mission-based computation, but also agent-based computation concurrently. The concept of an agent can be found in many different areas, particular in software engineering. MAS takes the notion of an agent further by allowing the agent to be autonomous (acting on its down), and also work within the construct of a *world*, where other agents may also exist and operate in a distributed manner. As computer systems become more distributed in- and of-themselves, does applying MAS to these systems become more attractive.

The authors of [14] view IoT as a cyber-physical-social complex network and implement a distributed multi-agent architecture to unify different IoT applications; they address the heterogeneity of IoT applications, enable them to interoperate with each other, make it efficient to introduce new applications, and enhance the flexibility and security of different applications (with a use case of smart home). In [15] conceptual MAS designs and architectures are proposed for applications in power systems and power engineering, where the authors state MAS are well suited to manage the size and complexity of these energy systems. The paper provides a broad look at control and operation of microgrids, with both application and limitations. The research in [16] also look at MAS for the Internet of Things (IoT). The authors discuss challenges of relevance to decentralized intelligence, including the heterogeneity of IoT components; asynchronous and delay-tolerant communication and decoupled enactment; and multiple stakeholders with subtle requirements for governance, incorporating resource usage, cooperation, and privacy. They also address possible research directions, including programming models, interaction-oriented software engineering, and governance. In [17], a multi-agent algorithm is devised to produced a distributed recommendation system in IoT environment. The output is an organized overlay-network of cyber agents that provides a way to obtain an efficient "things" recommender system. The authors of [18] contend that developers of MAS often fail to comply with strict timing constraints (crucial for safety-critical domains such as healthcare and automotive). In their paper they move from sole theory to provide an analysis of MAS components to comply with strict timing constraints, to better enable reliability and predictability. In [19], the authors' research attempts to enable construction of a globally-optimized social system by using new multi-agent algorithms that employ pricing mechanisms, matching mechanisms, and scoring mechanisms.

Much of today's research into MAS involve using the MAS itself to affect change in the actual system. In this context, the

MAS is not separate from the system, but rather *is* the system. Our research differs from others in that we approach the MAS not as an enabler for the system, but as a decoupled component that serves the system. The same way a computer may serve a user to do multiple different functions. An agent may exist on that computer to ensure the computer's resource are properly allocated. Our research is not to ensure the OT/IT/IoT network is functioning, but rather to ensure it is secure from attack.

V. Building a MAS: Technical Approach

Several approaches to better secure I/OT devices and infrastructure have been proposed. Many rely on solutions that cannot be reasonably implemented due to legacy equipment, vendor complicity, or cost. Corollary networks to I/OT are cloud networks, whose devices operate in the open-Internet, accessible by untrusted entities. The security paradigm in these networks has largely been based on agents, and have reaped successes. We apply the notion of agents in I/OT networks through security and mission decoupling. For those networks whose devices are fixed, Autonomous Agents (AA) will not require installation on the endpoints, but may integrated into the I/OT network-space (tied to a shared fieldbus, wireless network, or via bump-in-the-wire). For those that are software-based, an AA may be installed in user-space. AAs may provide:

1) Passive listening/active probing (where applicable)
2) Data/metadata collection
3) Behavioral analysis and majority voting schemes
4) AA self-policing
5) Active defense techniques
6) Security policy enforcement

The goal being that the AA/MAS shall not affect the real-time communication requirements of the system (ICS), nor the functionality of the devices (IoT). Leveraging multiple sources from academia and industry [20] [21] [22] [23] [24] [25] [26], we devised a generalized architecture of typical cyber-physical-enterprise networks that can address the constructs of legacy networks, is malleable to fit IoT network, and extendable to fit other network types (enterprise, cloud, mobile, tactical), with the option to adapt to future operations and management models as needed [27] [28] [29]. The mapping of the different network models to our generalized architecture is show in Table I.

The mission architecture S_n (1) describes the network where data or commands are pushed-to or pulled-from a Control tier C, to a Distribution tier D, and finally to a Physical tier P; business-oriented operations B connect to C. External entities E exist outside of the purview of S_n, and are adjacent to B. The underlying communication planes, or links L (2), are described broadly by the connections between the tiers.

$$S_n = \langle E, B, C, D, P \rangle \tag{1}$$

$$L = \langle l_{eb}, l_{bc}, l_{cd}, l_{dp} \rangle \tag{2}$$

TABLE I
Network Mappings

Model	B-Tier	C-Tier	D-Tier	P-Tier
ICS	Business, Logistics (Level 4)	Control software, HMI, Operations (Level 2/3)	Remote devices, collection (Level 1/2)	Physical domain, devices (Level 0/1)
IoT	Business, User Access (*Actions*)	Storage, Processing, Reporting, Cloud (*Insights*)	Gateways, Hub	Things, sensors
IIoT	Business Integration	Information, operations, applications	Control	Proximity & physical systems
Enterprise	Data center, edge, cloud	Core routing, boundary	Concentrator, distribution	Access, mobile, endpoints

In the C tier, operational devices collect data from or control devices in the P tier. The D tier provides the aggregation, normalization, filtering or summarization of data from devices in the P tier, any may also send command and control signals to the P tier endpoints. Devices in the P tier interact directly with their environment, either sensing or performing physical actions. Leveraging [30] as a foundation, the AAs interface directly with the P tier (on the broadcast medium, last physical hop or as an embedded agent), and the C, D, B tiers, to form a cogent MAS Agent Platform (AP) S_a (3), as a self-policing out-of-band network. Agents in the B tier may collect data, or serve as a Directory Facilitator (DF) nameserver ns_i for the S_a. Overall MAS control, developer/maintainer interface, and data push-pull mechanisms are handled by the Agent Management System (AMS), ams (where more than one may exist in the environment).

$$S_a = \langle a_{\{b,c,d,p\}}, ns_i, ams_i \rangle \tag{3}$$

The distributed agents in C, D and P (and B as required) collect data, correlate as needed, learn, and send summary or raw data to a AMS for additional reasoning, or may interface with an OT safety system to provide alerting for anomalous observations between the P, D and/or C tiers.

Given the proximity and interfacing with the operational environment, cybersecurity features may be integrated directly into the agents $a_{\{b,c,d,p\}}$ and nameserver ns_i to effect change as necessary. The feasibility of integration and operational responses are wholly dependent on the target environment. However, the decoupled nature of S_n and S_a provide the ability to update/include cyber responses leveraging $a_{\{b,c,d,p\}}$ as the delivery conduit. Each agent a_i is comprised of several components:

κ = developer/AMS knowledge
σ = sensor(s)
α = actuator(s)
ρ = percept
ν = neighbors

γ = goal(s)
kb = knowledge base

A percept may be drawn from sensors, information from neighbors, and actuator feedback (if applicable). The collection of all percepts over the time of the agent's life is the *percept sequence*. In order to achieve goals, the agent acts on retrieved percepts from sensors and refers to its knowledge base (4) to decide on the appropriate action.

$$kb = \sum_{i=1}^{\infty} \rho_i + \sigma + \kappa \tag{4}$$

Agents communicate via a Message Transport Service (MTS), that may be supported by S_n through L, or an alternate transport network. Agent Communication Language (ACL) [30] provides a rich set of message parameters to describe message context; the Communicative Act (CA) defines communications in terms of a function or action (as based on speech act theory), e.g. *accept proposal*, *agree*, *subscribe*, etc. Semantic Language (SL) is then used to define semantics for a CA as a logic of attitudes and actions; expressions are defined by *action expressions* or *propositions* which in turn are represented as well-formed-formulas (*wff*). This allows the ACL to facilitate a large vocabulary to describe the desires, beliefs, requests and replies between agents.

With sensing, actuation, communication and language available for agents, the next step in this research is to define the knowledge, goals, and environmental features for the MAS.

VI. Conclusions and Future Work

Protecting devices in the cyber-physical domain is dire to the safety, security, and privacy of a nation and its citizens. Most proposed solutions tend to the safe-path by attempting to deploy solutions that often only work with unconstrained computing devices. In this paper we have proposed employing a Multi-agent System (MAS) architecture to promote cybersecurity through sensing and actuation in an I/OT network. Currently, efforts are underway to implement the specification in a simulated/emulated environment for initial test and evaluation. The results of which shall be covered in another research paper, to include follow-up work regarding parameterization of cyber sensing and actions based on data-types, and dynamic policy enforcement.

References

[1] W. M. S. Stout and V. E. Urias, "Challenges to securing the Internet of Things," 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Orlando, FL, 2016, pp. 1-8.

[2] M. J. Haber, B. Hibbert, Industrial Control Systems (ICS). In: Privileged Attack Vectors. Apress, Berkeley, CA, 2018.

[3] A. Ginter, "The Top 20 Cyber Attacks Against Industrial Control Systems," White Paper, Waterfall Security Solutions, 2017.

[4] Anon, "The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History," 2017, https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

[5] J. Wallen, "Five nightmarish attacks that show the risks of IoT Security," 2017, https://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/

[6] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84, 2017.

[7] M. Lesk, "The New Front Line: Estonia under Cyberassault," in IEEE Security & Privacy, vol. 5, no. 4, pp. 76-79, July-Aug. 2007.

[8] A. Nadkarni, "Software-defined OT is here - the emergence of Converged IT/OT systems," 2017, https://idc-community.com/groups/it_agenda/infrastructureanddatamanagement/software_defined_ot_is_here_the_emergence_of_converged_itot_systems

[9] L. O'Donnel, "HPE Leads The Charge In IoT With New Software-Defined Operational Technology," 2017, https://www.crn.com/news/internet-of-things/300086536/hpe-leads-the-charge-in-iot-with-new-software-defined-operational-technology.htm

[10] P. Goldstein, "HPE Discover 2017: HPE Makes Operational Technology Software-Defined to Help Analyze IoT Data," 2017, https://biztechmagazine.com/article/2017/06/hpe-discover-2017-hpe-makes-operational-technology-software-defined-help-analyze

[11] S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach Upper Saddle River (New Jersey, 1995).

[12] H. Nwana, Software agents: an overview. The Knowledge Engineering Review, Vol 11:3, 205-244, 1996.

[13] Alonso, Eduardo. "From Artificial Intelligence to Multi-Agent Systems: Some Historical and Computational Remarks," Artificial Intelligence Review 21.1, 3-24, 1998.

[14] X. Liu, A. Leon-Garcia, and P. Zhu. A distributed software-defined multi-agent architecture for unifying iot applications. In 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pages 49–55, Oct 2017.

[15] Abhilash Kantamneni, Laura E. Brown, Gordon Parker, and Wayne W. Weaver. Survey of multi-agent systems for microgrid control. Engineering Applications of Artificial Intelligence, 45:192 – 203, 2015.

[16] M. P. Singh and A. K. Chopra. The internet of things and multiagent systems: Decentralized intelligence in distributed computing. In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pages 1738–1747, June 2017.

[17] A. Forestiero. Multi-agent recommendation system in internet of things. In 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pages 772–775, May 2017.

[18] Davide Calvaresi, Mauro Marinoni, Arnon Sturm, Michael Schumacher, and Giorgio Buttazzo. The challenge of real-time multi-agent systems for enabling iot and cps. In Proceedings of the International Conference on Web Intelligence, WI '17, pages 356–364, New York, NY, USA, 2017. ACM

[19] T. Ito, S. Chakraborty, R. Kanamori, and T. Otsuka, "Innovating multiagent algorithms for smart city: An overview," In 2012 Fifth IEEE International Conference on Service-Oriented Computing and Applications (SOCA), pages 1–8, Dec 2012.

[20] ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod): Enterprise-Control System Integration Part 1: Models and Terminology (2010)

[21] T. J. Williams (1993) "The Purdue enterprise reference architecture." Proceedings of the JSPE/IFIP TC5/WG5. 3 Workshop on the Design of Information Infrastructure Systems for Manufacturing.

[22] Industrial Internet Consortium, The Industrial Internet of Things Volume G1: Reference Architecture, IIC:PUB:G1:V1.80:20170131, 2017.

[23] Microsoft, Microsoft Azure IoT Reference Architecture Version 2.0, White Paper, 2018.

[24] IBM, Internet of Things architecture overview, IBM Cloud Architecture Center, 2018, https://www.ibm.com/cloud/garage/architectures/iotArchitecture/reference-architecture/

[25] Cisco Networks, Enterprise Campus 3.0 Architecture: Overview and Framework, 2008, Cisco Systems, Inc., San Jose CA.

[26] Juniper Networks, Reference Architecture: Midsize Enterprise Campus Design, White Paper, 2016.

[27] Conrad, "The Collapse Of The ISA95 Manufacturing Operations Management Model," 2014, http://www.manufacturing-operations-management.com/manufacturing/2014/09/the-collapse-of-the-isa95-model-for-manufacturing-systems.html

[28] G. Mintchell, Purdue Enterprise Reference Architecture Meets IIoT, 2016, https://themanufacturingconnection.com/2016/03/purdue-enterprise-reference-architecture-meets-iiot/

[29] Y. Lu, F. Riddick, N. Ivezic, "The Paradigm Shift in Smart Manufacturing System Architecture," In Nääs I. et al. (eds) Advances in Production Management Systems. Initiatives for a Sustainable World. APMS 2016.

[30] Foundation for Intelligent Physical Agents (FIPA), FIPA Abstract Architecture Specification SC00001L, 2003.