Architecting the next generation of service-based SCADA/DCS system of systems

Stamatis Karnouskos* and Armando Walter Colombo†

*SAP Research, Germany Email: stamatis.karnouskos@sap.com
†Schneider Electric and University of Applied Sciences Emden/Leer, Germany. Email: awcolombo@et-inf.fho-emden.de

***Abstract*—SCADA and DCS systems are in the heart of the modern industrial infrastructure. The rapid changes in the networked embedded systems and the way industrial applications are designed and implemented, call for a shift in the architectural paradigm. Next generation SCADA and DCS systems will be able to foster cross-layer collaboration with the shop-floor devices as well as in-network and enterprise applications. Ecosystems driven by (web) service based interactions will enable stronger coupling of real-world and the business side, leading to a new generation of monitoring and control applications and services witnessed as the integration of large-scale systems of systems that are constantly evolving to address new user needs.**

I. Introduction

Industrial processes as well as many modern systems depend on SCADA and DCS systems in order to perform their complex functionality. Typical examples include electric power grids, oil refining plants, pharmaceutical manufacturing, water management systems etc.; the main tasks they perform are monitoring and control over a highly diversified infrastructure. Monitoring and control (M&C) heavily depends on the integration of embedded systems, and is expected to grow from 188€ Bn in 2007, by 300€ Bn, reaching 500€ Bn in 2020 [1]. This will have a significant impact in several domains and especially in vehicles, manufacturing and process industry, as well as healthcare and critical infrastructures.

As we move towards and infrastructure that increasingly depends on monitoring of the real world, timely evaluation of data acquired and timely applicability of management (control), several new challenges arise. The latter is becoming even more difficult when one considers the prevailing Internet of Things, where practically networked embedded devices are integrated not only in industrial domain but in every aspect of our life. As such the data points that need to be monitored and controlled increase rapidly, and so are the requirements for high performance monitoring and analytics as well as efficient management.

Current SCADA/DCS systems architectures were designed for more closed and controlled industrial environments, however it is expected that there is potential to enhance their functionality and minimize integration costs by integrating themselves into collaborative approaches with enterprise systems and large-scale real-world services. As environments become more complex, it is not anymore viable (e.g. cost-/time-wise) to engineer individual self-contained systems but rather integrate large-scale Systems of Systems (SoS). We need to consider what the next steps could be towards engineering/designing the next generation of SCADA/DCS systems of systems that could successfully tackle the emerging challenges such as degree of centralization, optional independence of each of the participating systems, and independent evolution of them [2] [3].

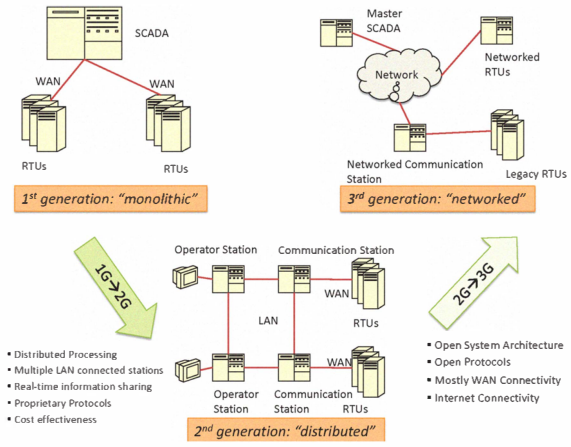

Figure 1. SCADA system evolution

II. SCADA/DCS systems

A typical SCADA System consists of several subsystems notably:

- A Human-Machine Interface (HMI) where the information is depicted and is used by human operators to monitor and control the SCADA linked processes.
- A computer which does the monitoring (gathering of data) as well as the control (actuation) of the linked processes
- Remote Terminal Units (RTUs) which collect data from the field deployed sensors, make the necessary adjustments and transmit the data to the monitoring and control system
- Programmable Logic Controllers (PLCs) that are used as an alternative to RTUs since they have several advantages over the special-purpose RTUs
- A communication infrastructure connecting all components

As depicted in Figure 1, we have witnessed the last decades a shift in the architecture of SCADA systems [4]. In the

978-1-61284-972-0/11/$26.00 ©2011 IEEE

first generation we had monolithic systems connected via a WAN to the RTUs at the place of action. However in the second generation we moved towards a more distributed flavor where LAN was used to interconnect the components. This approach was more cost effective than the first generation and allowed distributed processing and real-time information sharing among the entities based on proprietary protocols. The emergence of the third generation moved towards utilizing the network as such, using not only WAN but also Internet, and featured an open system architecture and open protocols. The next generation will push further the limits in the network, albeit taking advantage of integrating and composing the SCADA-SoS from capabilities provided by large-scale participating systems, which no longer have a single controlling/management authority, have components that are developed and evolve independently, and are using several emergent technologies in hardware and software, as we depict later in section IV.

Similarly a DCS system is composed of functionally and/or geographically distributed controller elements that are interconnected by a communication network for monitoring and control. However depending on the functionality addressed, these two can differ. It is not uncommon that tasks can be performed both well by a SCADA and a DCS system, however in industrial reality few usages have been designed with this in mind; as a result real-world integration usually brings up the differences such as data timely availability. As an example a DCS system has a process oriented view, while a typical SCADA system is more data acquisition oriented. Generally SCADA systems are expected to operate reliably over unreliable links (but always keep a backlog of acquired data), while DCS systems have direct access to the source of data and therefore the latest values. Additionally SCADA systems are mostly event-driven while DCS systems generally run sequentially. The last for instance has an effect on alarm generation i.e. on event for SCADA but at process state change for a DCS.

We must point out however that the last years both SCADA and DCS systems have come together and nowadays share more common ground than ever. This is attributed to the advances in communication and computation that can be delivered by networked (embedded) systems, industrial PCs and the application of new paradigms like the Service-oriented Architecture (SOA) and System-of-Systems (SoS) [5]. Several other ongoing software and hardware trends will further impact the evolution of the two, effectively leading to a new system of systems; as such we will consider any further reference to SCADA/DCS in this paper.

III. Technology Trends

Modern enterprises need to be agile and dynamically support decision making processes at several levels. For this to work out, critical information need to be available at the right point in a timely manner at several levels. Especially with cross-layer collaboration in mind, providing fine grained info when it is needed and in the right form is a challenging task. In the future infrastructures where a huge amount of data is generated by real world devices and needs to be integrated, processed within a specific context and communicated on-demand and on-time, traditional approaches aiming at the efficient data inclusion in enterprise services need to be changed.

A. Information Driven Interaction

Integration with business systems is done at an inflexible and usually business-relevant agnostic way – relevant only to the communication of specific data, but without a clear matching or even estimation of the effect on the business side. Furthermore due to the deployment of isolated and task specific solutions, we have ended up with infrastructures that are not interoperable, can not collaborate because of data-understanding barriers and even communication difficulties although e.g. physical proximity could in theory make that possible. The result is the existence of several horizontal and vertical media breaks, that are patched up with proprietary solutions and gateway/tunneling approaches that complicate things further.

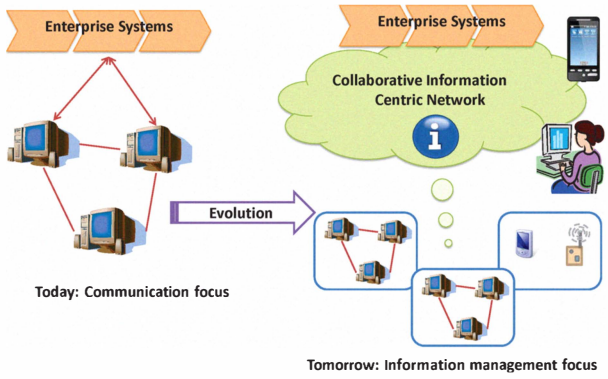

Figure 2. IT trend: information driven interaction

In such a mixed, non-standardized and highly complex infrastructure, business applications have a very hard way to dynamically discover, integrate, and interact with the sensing/actuating devices although this is wished. Vice versa, the device world has very little chance of fostering intra-/inter- collaboration capabilities and take advantage of the opportunity to offer their functionality in tight interaction with enterprise functionalities.

As such the move towards an information driven network rather than a communication one is needed (as depicted in Figure 2). The service oriented architecture (SOA) paradigm points us towards a potentially right direction. By abstracting from the actual underlying hardware and communication-driven interaction and focusing on the information available via services, we move towards a service driven interaction. Services can be dynamically discovered, combined and integrated in mash-up applications.

B. Distributed Business Processes

In a world envisioned by the Internet of Things where millions of devices cooperate and offer open access to their functionality, and where the Internet of Services allows the creation of mash-ups that mix and integrate the virtual and real world, electronic business services can benefit tremendously from their combination. In such large scale infrastructures, tunneling of data to back-end systems or centralized databases is not a viable solution for the majority of scenarios. Enterprise systems trying to process such a high-rate of non- or minor relevancy data, will be overloaded. As such the first strategic step is to minimize communication with enterprise systems only to what is business relevant. Thus information needs to be processed at local loops and be explicitly propagated. Correlation of information and cooperation scenarios in a goal oriented way is needed.

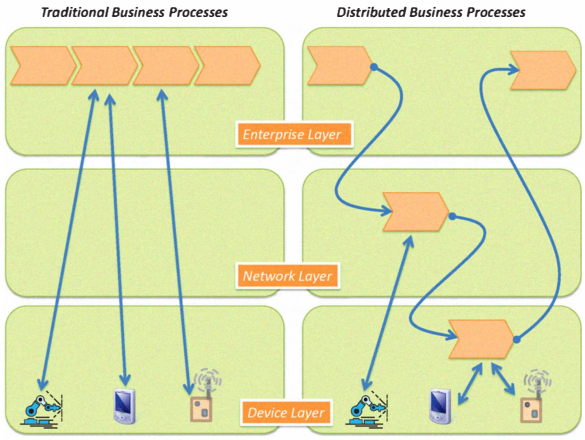

Figure 3. Distributed Business Processes on-device and in-network

The next step is to partially outsource functionality traditionally residing in enterprise systems to the network itself and the edge nodes. As devices are increasingly capable of computing, they can either realize the task of processing and evaluating business relevant information they generate by themselves or in clusters (as depicted in right part of Figure 3). The business process can now be by design distributed, where parts of the required functionality are executed at the item itself e.g. on-sensor or in-network (e.g. sensor networks and/or other services provided by independent service vendors). Distributing load in the layers between enterprises and the real world infrastructure is not the only reason; distributing business intelligence is also a significant motivation.

C. Cooperating Objects

The rapid advances in computational and communication part in embedded systems, is paving the way towards highly sophisticated networked devices that will be able to carry out a variety of tasks not in a standalone mode as usually done today, but taking into full account dynamic and context specific information. These "objects" will be able to cooperate, share information, act as part of communities and generally be active elements of a more complex system. The domain of Cooperating Objects [6] is a cross-section between (networked) embedded systems, ubiquitous computing and (wireless) sensor networks.

An initial definition coming from the European Commission co-funded project CONET states [6]: Cooperating Objects consist of embedded computing devices equipped with communication as well as sensing or actuation capabilities that are able to cooperate and organize themselves autonomously into networks to achieve a common task. The vision of Cooperating Objects is to tackle the emerging complexity by cooperation and modularity. Towards this vision, the ability to communicate and interact with other objects and/or the environment is a major prerequisite. While in many cases cooperation is application specific, cooperation among heterogeneous devices can be supported by shared abstractions.

We expect that next generation SCADA/DCS systems will take advantage of such emergent behavior and integrate it in their functionality. As such the governing logic may be expressed in a goal oriented manner assigned to communities of cooperating objects aiming at satisfying business process requirements.

D. Virtualization and Cloud Computing

In the IT world we witness a trend towards virtualization of resources such as a hardware platforms, operating systems, storage devices, network resources etc. Virtualization addresses many enterprise needs for scalability, more efficient use of resources, and lower of Total Cost of Ownership (TCO) just to name a few. Cloud Computing is emerging powered by the widespread adoption of virtualization, service-oriented architecture and utility computing. IT services are accessed over the Internet and local tools and applications (usually via a web browser) offer the feeling as if they were installed locally. However the important paradigm change is that the data is computed in the network but not in a priori known places. Typically physically infrastructure is not owned and various business models exist that consider access oriented payment for usage. This IT trend impacts already IT applications, however it may also affect how industrial applications are designed in the future and how they integrate with externally offered services.

E. Multi-core systems and GPU computing

Most of industrial systems are built for the long-term and with proven technologies. However since 2005 we have seen the emergence of multi-core systems, that nowadays exist also in normal smartphones. The general trends is towards chips with tens or even hundreds of cores. Advanced features such as simultaneous multi-threading, memory-on-chip, etc. promise high performance and a new generation of parallel applications unseen before in embedded systems. Additionally in the last decade we have seen the emergence of GPU computing where computer graphic cards are taking advantage of their massive floating-point computational power to do stream processing. For certain applications this may mean a

performance increase to several orders of magnitude when compared with a conventional CPU.

Furthermore a recent trend of integrating built-in graphics capabilities with processors (graphics-enabled microprocessors – GEM) like Intel's Sandy Bridge and AMD's Fusion, may imply that capabilities of GPU computing may be available to any kind of device hosting one of those processors. Such a CPU/GPU hybrid can possibly be even more efficient by removing the slow communication between CPU and GPU. The processors with built-in graphics capabilities to be installed in 2011 on 115 million notebooks accounts for half of total shipments, and on 63 million desktop PCs which accounts for 45% of the total number. By 2014, 83% of the world's notebooks and 76% of desktops will ship with graphics-enabled microprocessors [7].

Multi-core and GPU computing will have an impact on existing design of SCADA/DCS systems as now more sophisticated approaches can be deployed, and for instance analysis of processes, production and resources can be done in a costly effective manner even at the point of action and not on the master SCADA system as traditionally done according to the evolution shown in Figure 1.

F. SOA-ready devices

In the future, a much more diversified infrastructure will emerge, and the way we interact with it will change significantly. A mash-up of services will be created, that can be combined and used in a cross-layer way. Enterprise applications will be able to connect directly if needed to devices, without the use of proprietary drivers, while non-web-service enabled devices can still be attached and their functionality wrapped by service mediators or at middleware layer [8]. Peer to peer communication among the devices is already pushing SOA concepts down to device layer and create new opportunities for functionality discovery and collaboration as demonstrated [8].

Networked embedded systems have become more powerful with respect to computing power, memory, and communication; therefore they are starting to be built with the goal to offer their functionality as one or more services for consumption by other devices or services. Due to these advances we are slowly witnessing a paradigm shift where devices can offer more advanced access to their functionality and even host and execute business intelligence, therefore effectively providing the building blocks for expansion of service-oriented architecture concepts down to their layer. As such, event based information can be acquired, processed on-device and in-network, without the need of storage in intermediate databases and processing by third parties, and eventually be conveyed to the corresponding business processes. This capability provides new ground for approaches that can be more dynamic and highly sophisticated, and that can take advantage of the context specifics available.

Web services are suitable and capable of running natively on embedded devices, providing an interoperability layer and easy coupling with other components in highly heterogeneous shop-floors [8], [9]. Device Profile for Web Services (DPWS) and OPC UA are emerging technologies for realizing web service enabled controllers and devices. Several projects such as SIRENA (www.sirena-itea.org), SODA (www.soda-itea.org) and SOCRADES (www.socrades.eu) have experimented with SOA-ready industrial automation devices and their integration on industrial applications.

IV. Next Generation SCADA/DCS

We have explored several IT trends that we consider may significantly change the way we design, implement and deploy industrial applications in the future. The next generation SCADA/DCS systems will have to cope with a much higher amount of diverse distributed data and information in real-time and make decisions based on cooperation with internal and external data and information acquired and exposed as "services".

A. Vision

A vision of how the next generation SCADA/DCS systems may look is depicted in Figure4. We can identify the following main changes to the whole infrastructure: it is now information driven and all interactions are done via (web) services in a flat form. From the SOA view point, all the systems (e.g. ERP, PLCs, legacy SCADA/DCS, devices, MES etc.) expose their functionality (complex or atomic) as a service that can be composed by and interact with other entities. Logic is hosted where is makes (business) sense e.g. near to the point of action (device level) or even distributed (in several layers).

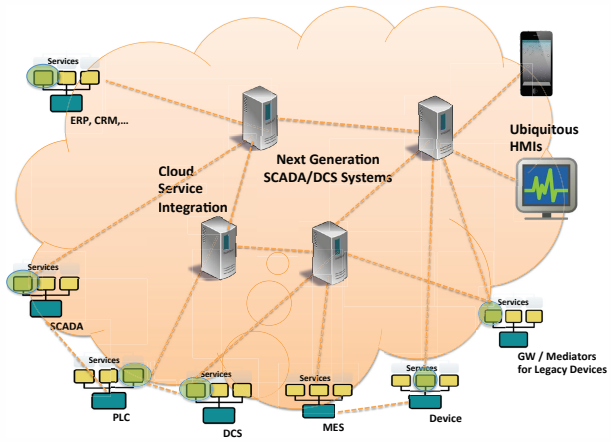

Figure 4. Next Generation SCADA/DCS system vision – flat information-driven interaction

The HMI is no longer attached to a static location, but accessible from anywhere and any time via any (mobile) device. Additionally its functionality is not monolithic, but composed as a mash-up application from services [10] hosted on-device and in-network (e.g. in cloud).

The monitoring of data as well as the control of the linked processes is done in a collaborative manner. Actually in-cloud powerful services can deliver high performance analytics on

the monitored data and hosted decision support systems can analyze real time data coming not only from the shop-floor but also interconnected business processes.

RTU functionality is now embedded in service mediators or even directly in intelligent devices which now report directly over the network the collected data to the distributed monitoring and control system. Depending on the capabilities offered by the devices, the data can also be preprocessed matching exactly the requirements expected by the monitoring system, without having to transmit unnecessary information.

PLCs are now multi-core and can execute sophisticated logic or even precompute on real-time streams e.g. based on embedded low cost GPUs. PLC services can be on-the fly updated or adjusted depending on the horizontal and vertical collaborations it takes part e.g. with the SOA-based enterprise levels.

A communication infrastructure connecting all components is still the backbone, however it is much more diversified over several wired and wireless channels, providing QoS depending on the application's dynamic needs. The introduction of Internet technologies everywhere and service based interactions ease the integration and interoperability, leading to lower total cost of ownership and rapid deployment of highly customized solutions.

We expect that the next generation SCADA/DCS systems will be an integral part of a large ecosystem of people, devices, processes that need to collaborate in order to achieve goal-driven targets. Complex key performance indicators (KPIs) will enable an unprecedented scale of assessing in real time the status at any layer, evaluate alternatives, and adjust resources (infrastructure, processes, people action etc.) in order to deliver optimal performance.

The future "Perfect Plant-Wide System" [9], [11] will be able to seamlessly collaborate and enable monitoring and control information flow in a cross-layer way. The different systems will be part of a SCADA/DCS ecosystem, where components can be dynamically added or removed and dynamic discovery enables the on-demand information combination and collaboration. All current and future systems will be able to share information in a timely and open manner, enabling an enterprise-wide system of systems [12] that will dynamically evolve. As all systems will be more "fluid" and loosely coupled, we expect an easy upgradeable infrastructure that can co-evolute with the emerging business needs; this will enable us to design today the perfect "legacy" system of tomorrow, which will be able to be easily integrated in long-running infrastructures (e.g. the pharmaceutical one with lifetime of 15-20 years).

Finally we have to point out clearly, that the next generation SCADA/DCS systems may not have a physical nature. This implies that it might reside only on the cyber or "virtual"world, in the sense that it will comprise of multiple real world devices, on-device and in-network services and collaboration driven interactions, that will compose a distributed highly agile collaborative complex system of systems.

B. Considerations & Future Directions

SCADA/DCS systems are increasingly important for various domains e.g. manufacturing, process industry, as well as critical infrastructures such as the SmartGrid, Intelligent Transportation Systems etc. Considering the trends and visions depicted here, we consider that key directions should be investigated, while considering a complex collaborative ecosystem of interacting devices, systems and entities.

Monitoring: Monitoring of assets is of key importance especially in a highly complex heterogeneous infrastructure. In large scale systems it will be impossible to still do the information acquisition with the traditional methods of pulling the devices. The more promising approach is to have an event driven infrastructure coupled with service-oriented architectures. As such any device or system will be able to provide the information it generates (data, alarms etc.) as an event to the interested entities and will also be able to compose, orchestrate that information/services in a model-based manner, generating new monitoring indexes not envisioned at the design stage of the composing systems (typical characteristic/property of SoS).

Management and Visualization: The next generation factory systems will be composed of thousands of devices with different hardware and software configurations. It will be impossible to continue managing such infrastructures the way we do it today. We will need to automate as much as possible primarily the monitoring part and also the soft-control of such systems. As such it should be possible to dynamically discover devices, systems and services offered by the infrastructures. It should be possible to do software upgrades and mass reprogramming or re-configuration of whole systems. Additionally (remote) visualization [10] of the real infrastructure is a must as it will give the opportunity of better understanding and maintaining it. The increased complexity will not allow per device management, therefore self-* features are desirable, at least at system level. More specifically self-configuration (automatic configuration of components), self-healing (automatic discovery, and correction of faults), self-optimization (automatic monitoring and control of resources to ensure the optimal functioning with respect to the defined requirements) and self-protection (proactive identification and protection from arbitrary attacks) might ease large scale management and maintenance.

Security, Trust and Privacy: As next generation SCADA/DCS system will heavily interact with other systems (and in cloud services), apart from ongoing complex security concern [13], additional issues related to proper security, trust and privacy need to be investigated. We consider mostly today that all devices and systems are operated under the same authority or the same user. However this might not hold true in the future. Systems may be composed from simpler ones that may be administered by different entities and possibly not under the same security domain.

Scalability: Scalability is a key feature for large scale systems. For industrial systems it is expected that scaling up of resources available on single devices will emerge anyway.

As such the impact should be considered e.g. at SCADA/DCS etc. in order to assess what capabilities can be assumed by large scale applications e.g. monitoring. Scaling out is also a significant option to follow, especially relevant to nodes having attached a large number of devices e.g. a SCADA system or even a monitoring application running in the cloud with thousands of metering points.

Real-time Information Processing: We anticipate that the real-time information acquisition is a challenging task, however for next generation applications to be able to react timely, we also need real-time information processing. The latter includes possible pre-filtering or pre-processing of information for a specific (business) objective and complex analysis of relevant (stream) events. Since real-time event processing relies on several steps, we need to tackle the challenges raised by them such as event-pattern detection, event abstraction, event scheduling, event filtering, modeling event hierarchies, detecting relationships (such as causality, membership or timing) between events, abstracting event-driven processes etc.

Mobility Support: The recent advances in mobile devices have already led to significant changes in the way business is conducted. Especially in customer interactions but also in industrial processes such as maintenance new approaches can be adopted where workers fully equipped with on-demand real time information can interact via mobile devices with business systems as well as local devices. We need to investigate the support for mobile devices e.g. being used as HMIs, the support for mobility of devices i.e. where devices are themselves mobile and the implications of this, the support for mobile users and interaction with static and mobile infrastructure, the support for mobility of services e.g. where services actually migrate among various infrastructures and devices following e.g. user's profile constraints.

Simulation: Industrial environments are complex systems of systems. As such any change to a part of them may have unexpected results in other depending or collaborating parts. However independent evolution of smaller systems are a must to achieve adaptivity and evolvability. As such a system emulation is highly needed in order to be able to identify early enough possible conflicts and side-effects. Such simulations may be used in pre-deployment time: evaluation of behavior of changes to be applied and monitoring of them, as well as after deployment and during runtime.

Interoperability: As next generation systems will be highly collaborative and will have to share information, interoperability via open communication and standardized data exchange is needed. System engineering of complex interoperable systems has profound impact on their evolution, migration and future integration with other systems. The future industrial infrastructure is expected to be constantly evolving. As such it is important to be (i) backwards compatible in order to avoid breaking existing functionality as well as (ii) forward compatible which implies designing interfaces and interactions as rich as possible with possible considerations on future functionality to come.

V. Conclusion

We are still at the begin of an era where complex system of systems will further blur the fabric of business and physical worlds. Monitoring and Control will be of key importance for any real-world application and as such systems and services involved have to be able to handle the upcoming heterogeneous large-scale infrastructures. We have presented some major trends that will reshape the way we design, implement and interact in future industrial environments, especially when it comes to monitoring and management. The IT-driven technology trends pose new challenges and open up new opportunities; however this will need to be supported by a next generation of highly sophisticated SCADA/DCS systems of systems. We elaborate on some considerations when designing such systems, and present what we consider the future SCADA/DCS may look like.

Acknowledgment

The authors would like to thank for their support the European Commission, and the partners of the EU FP7 projects IMC-AESOP (www.imc-aesop.eu) and CONET (www.cooperating-objects.eu) for the fruitful discussions.

References

[1] "Monitoring and control: today's market, its evolution till 2020 and the impact of ICT on these," European Commission DG Information Society and Media, Oct. 2008. [Online]. Available: http://www.decision.eu/smart/SMART_9Oct_v2.pdf

[2] S. Karnouskos, A. W. Colombo, F. Jammes, J. Delsing, and T. Bangemann, "Towards an architecture for service-oriented process monitoring and control," in *36th Annual Conference of the IEEE Industrial Electronics Society (IECON-2010), Phoenix, AZ.*, 7–10 Nov 2010.

[3] G. A. Lewis, E. J. Morris, P. Place, S. Simanta, D. B. Smith, and L. Wrage, "Engineering systems of systems," in *2nd Annual IEEE Systems Conference, 7-10 April, Montreal, Canada*, 2008.

[4] "Supervisory Control and Data Acquisition (SCADA) Systems," National Communications System (NCS), Technical Information Bulettin 04-1, Tech. Rep., Oct. 2004. [Online]. Available: http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

[5] S. Simanta, E. Morris, G. Lewis, and D. Smith, "Engineering lessons for systems of systems learned from service-oriented systems," in *4th Annual IEEE Systems Conference, 5-8 April, San Diego, CA*, 2010.

[6] P. J. Marrón, S. Karnouskos, D. Minder, and A. Ollero, Eds., *The emerging domain of Cooperating Objects*. Springer, 2011.

[7] R. Jennings, "Analyst: Nearly half of all pcs to use graphics processors," online, Mar. 2011. [Online]. Available: http://www.techworld.com.au/article/380121/analyst_nearly_half_all_pcs_use_graphics_processors/

[8] S. Karnouskos, D. Savio, P. Spiess, D. Guinard, V. Trifa, and O. Baecker, "Real World Service Interaction with Enterprise Systems in Dynamic Manufacturing Environments," in *Artificial Intelligence Techniques for Networked Manufacturing Enterprises Management*. Springer, 2010.

[9] A. W. Colombo and S. Karnouskos, "Towards the factory of the future: A service-oriented cross-layer infrastructure," in *ICT Shaping the World: A Scientific View*. European Telecommunications Standards Institute (ETSI), John Wiley and Sons, 2009, vol. 65-81.

[10] D. Idoughi, M. Kerkar, and C. Kolski, "Towards new web services based supervisory systems in complex industrial organizations: Basic principles and case study," *Comput. Ind.*, vol. 61, pp. 235–249, April 2010.

[11] P. Kennedy, V. Bapat, and P. Kurchina, *In Pursuit of the Perfect Plant*. Evolved Technologist, 2008.

[12] M. Jamshidi, Ed., *Systems of Systems Engineering: Principles and Applications*. CRC Press, Nov. 2008.

[13] N. Cai, J. Wang, and X. Yu, "SCADA system security: Complexity, history and new developments," in *6th IEEE International Conference on Industrial Informatics (INDIN)*, 2008.