Reusable Framework for Remote Monitoring and Maintenance of Manufacturing Systems

doi:10.3991/ijoe.v5i4.1024

J. Fayolle, C. Gravier, M. Ates
TELECOM Saint-Etienne, St. Etienne, France

***Abstract*—The aim of this paper is to address the problem of remote control of manufacturing systems for maintenance, object conception and production purposes.**

We present a global approach of this problem according to two research axis: the genericity of the platform according to the underlying device, and the security of the data and information systems. The primary goal of this paper is to describe the framework that allows the remote control, and especially its independence to the devices. We propose a special study on the security issues in such architecture by explaining why we have made the choice of adopting identity federation technologies as a mean to reach remote devices hosted in different Information Systems. We also describe how this kind of systems can be used in a collaborative way in order to build a real extended entreprise for e-manufacturing systems.

I. INTRODUCTION ABOUT REMOTE MONITORING AND MAINTENANCE OF MANUFACTURING SYSTEMS IN INDUSTRY

Manufacturing industry worldwide has been facing unprecedent challenges due to the globalization of markets, the increase of robustness and agility on the supply chains. This is also one consequence of the evolution of social demands, regional, governmental and environmental regulations. E-commerce and Internet technologies injected "velocity" into the front business activities and enabled companies to shift their manufacturing operations from the traditional factory integration philosophy to a supply chain-based e-factory philosophy. It transforms companies from a local factory focus to a global enterprise and business focus.

This concept is well define by Jay Lee in [15] as the concept of e-manufacturing : a new concept to answer the aforementioned needs of business strategies for complete integration of all business elements including suppliers, customer service network and manufacturing units by leveraging the Internet, web-enabling, tether-free technologies and computational tools. One of the main advantage of aim of e-manufacturing is the ability to monitor the plant floor assets, and predict the variation and performance loss for dynamic rescheduling of production and maintenance operations, and synchronize with other related business actions to achieve a complete integration between manufacturing systems and upper-level enterprise applications.Since the introduction of this concept in the earlier of this century, there is a lot of works that have been done in different scientific fields, mainly on the supply chain management (technology part and social part) and on the interoperability of information systems to smooth the difficulties of data exchanges.

However, from our point of view, the problem is not well posed. Indeed, many research papers deal with ``how can we improve the velocity of the products and data exchanges ?". With this approach, the assumption is that you have not the control on the remote systems and you are reduced to do your best with what is done on the other side.

The approach we propose in this paper is to show how to interact directly on the production systems or on the remote information systems in order to build a complete remote e-manufacturing system. Therefore, the objective of our work is to get the remote control on devices in order to design, build new products, but also for maintenance purpose.

In today's global competitive marketplace, there is intense pressure for manufacturing industries to continuously reduce and eliminate costly, unscheduled downtime and unexpected breakdowns. The aim is to change from transforming traditional "fail and fix (FAF)" maintenance practices to a "predict and prevent (PAP)" e-maintenance methodology [16]. This paper does not address here the prediction algorithm but the way we can prevent a fault through remote action on the manufacturing system. The challenge of a framework proposal is to allow the remote control of systems independently of the underlying device without breaking the strong industrial security considerations. Among the main technical challenges, we can cite the multiple standard, multiple operating systems, and the different security policies.

To sum up, the pillars of a reusable framework for remote monitoring and maintenance of manufacturing systems relies on:

- The heterogeneity of client devices,
- Geographical distributions of users and devices,
- The software development cost of e-manufacturing solutions adapted to each situation, each client device and each remote device.
- Ensure the data privacy of industrial firms (the remote control do not involve the loss of data in foreign systems and also do not induce some holes in the security policy of the information system).
- E-maintenance of devices safety.

If we want to promote the use of remote control for manufacturing systems, we have to address the above problems in a global approach. On the whole, these questions can be reformulated in the following way:

- The genericity of the framework according to the client device and according to the remote device,
- The security considerations: how to interact between peoples and devices which are very probably not authenticated in the same Information Systems
- The data integrity: no loss or no perturbation of data due to the remote exchange.

The paper is organized as follows. First, we address the problem of taking the control on a physical device through the Internet, focusing on device independence (a solution of remote e-manufacturing framework that is not supposed to be dedicated to the device it supports). Such an approach is also known as Remote Laboratories, and tries to cope with the lack of remote hands-on approaches within distance learning or remote services in industrial fields. Secondly, we deal with the consequences of such open door on the security of the Information System. We briefly explain how security federation can be the key for sharing devices between different firms and clients coming from different Information Systems) without breaking any security constraints. Finally, section 6 concludes.

II. RELATED WORKS

Since few years, the use of Internet as a way to build extended entreprise and take the control of remote manufacturing systems is growing very fast. One of the main research fields connected to this problem is Distance learning. Distance Learning has brought to the Web a number of learning tools, making lectures possible in the case of teachers and learners are in different place and/or at different time. We can used the results of theses scientific fields especially to deal with material object and not only insubstantial parts (cf. [10]) and therefore to build some tools in order to interact with manufacturing systems. The need of mobility and geographic spreading of exchanges adds a new dimension: the fact that one person is not coming all the time from the same point (geographical mobility) and is still wanting to be connected to its manufacturing systems. For most of current solutions, the approach is web based ([7, 23, 14, 20]), sometimes uses continue multimedia streaming [2] or integrated environments such as the set of Matlab toolkits [6]. Almost all of the actual solutions, however, are not adapted to transfer professional skills on real devices (for example, the way the device is supposed to be manipulated).

There is no denying that the use of a computer or a phone introduces a new media. But we have to assure that ``felt-life'' ([12, 19]) has also to be translated within the platform, for the computer link to be as transparent as possible. It is known that the productivity level is widely based on previous personal experiences : "this is principal means by which knowledge transitions from a declarative form (encoding of examples) to a procedural form (production rules)" [3]. What wa have to consider is to propose distant user interfaces wich is very close to the real ones. However, this aim is very hard to re-introduce in the context of remote control of device. This is why many schemes of e-manufacturing systems for extended entreprises only address the theoretical point of view, leaving the remote actions to physical sessions. Moreover, what we need is not to produce a way to remote control *one* device but a framework on which we can plug any kind of devices. In [13], the authors propose a Service Oriented Architectures to get the necessary modelisation in order to be adaptable to each kind of manufacturing devices.

The objective of our work is to demonstrate that we can build a generic and collaborative framework on which we can plug any kind of real and distance devices and control them through the Internet. The proposed framework has to be generic in the way that we do not want to redevelop the protocol of information exchange since, on the whole, the information are similar (commands, answers, parameters, ...). If we have to code this behavior independently for each device, this will be unsatisfactory, especially when the number of devices is large. As in the work developped by Hao in [13], the Framework we propose hereafter is based on a server side oriented architecture and a semantic modélisation of the manufacture devices.

Moreover, the use of remote control inside real process of manufacturing needs to validate that the remote part doesn't break security policies. The security question is rarely addressed by the research papers, or it is just the authentication part, such as in [18] which promoted a role-based access on a networked manufacturing systems. It is an evidence that through the opening of remote control, we may create security holes. Indeed, by thinking about the use of one device belonging to one firm, and which is proposed as a service to other ones, we have to allow the connection to people which are not known in the second Information System. In a paper dealing with e-health and e-business for m-commerce, the authors [22], put the focus on the same point : the issue of security, privacy, and integrity of information and transactions being exchanged from one point of the network to another is seen as a key barrier to making mobile solutions a reality.

To perform this, we have to build a solution which exchanges information about identities and security associated to these identities. An obvious solution is to work on the feeling of trust you get about people coming from this firm. Identity federation aims at creating Circles of Trust (namely CoT) between Information Systems sharing pre-established administrative bounds. It means to make the retrieval of the clearance of access from the Information System possible the requested digital identity belongs to. Identity federation means safely transport identity information in respect of users' privacy in an undefined environment, by taking care of privacy legislation according the domain of application[1]. In Liberty Alliance architectures, for example, users are asked to give their approval when a service provider requires identity attributes. Furthermore, federation architectures rely on pseudonymity [21] to support privacy.

The last criterion which is important for us in order to propose a real e-manufacturing systems is to assure that the system allows the collaboration between different users working on the same project or on the same remote device. As Lin said [17], the new challenge of enterprise interoperability is to share knowledge inter-business via networks to enable all partners to benefit and win in their markets. Its project envisages the delivery of collaborative knowledge services which increase inter-team awareness whilst improving coordination through moderation module, to achieve the global visions of enterprise interoperability.

[1] Two main references are two European directives: The Framework Data Protection Directive 95/46/EC (Directive) et The Electronic Communications Data Protection Directive 02/58/EC (ECDP Directive)

What we address here is how we can propose a solution which *group together the advantages of transparent and web based access to remote devices, unbreaking security policies and collaborative works*. According to the related Works presented above, we have found some partial solutions answering to one aspect of the problem, but the added value of our proposition is to deal with all the aspect at the same time. Many works have been done on the paradigm of remote control of devices. A survey of an important set of related works can be found in [10].

III. REMOTE CONTROL FRAMEWORK

A. On the reusability of remote manufacturing control systems

In 2000, we started researches on remote control of devices [5], based on a network Analyzer (a network analyzer allows the measurement of module and phase of reflected and transmitted signals of a device) and an antenna workbench we wanted to put online. These two devices have very different interaction protocols. The network analyzer is controlled trough buttons and charts, therefore physically static but induces electronic measurements and the antenna workbench conveys mechanical experiences (moving antenna and starting/stopping motors). The resulting Graphic User Interfaces (GUI), however, arevery close, because the GUI displays the same kind of widgets, whatever the device is (buttons, led, curves and charts, moving objects, menus, etc). Nevertheless, the commands are very different and for example, a button action induces some actions which are dependent of the device and of the *protocol* used to address the device. Besides, we become aware that we were about to reinvent the wheel each time we want another device online. This tends to illustrate that dedicated integrations are short term answers that are not supposed to be reused for other platforms involving other devices.

Moreover, since we want to exploit the proposed framework for remote control of very different manufacturing systems, the effort induces by putting online a new device has to be as less as possible. Another aspect is the centralization of such information system. Indeed, if the framework used for remote control is dedicated to one type of devices, the end of the story will be certainly the presence in the industry of many different frameworks, and then you will be face to another problem of e-maintenance: the maintenance of the frameworks themselves. Therefore, we have to propose a generic framework on which every kind of devices can be remote controlled without strong dedicated development.

In the context of Remote Manufacturing design, aiming at devices' independence means supplying interoperability tools, in order to get Remote Manufacturing platform able to support any kind of "remote-able" devices. Such an objective needs a formal representation of what a device is, qualifying the device with no more and no less details than necessary. To reach that goal, we need a representation of knowledge that allows to conceptualize a specific domain *and* to specialize (instantiate) that domain [11]. This way, the representation of the knowledge is shared among all devices, and each device goes with a specialization of that domain of knowledge. This requirement of interoperability perfectly fits the definition of ontologies (and one standard specification known as OWL[2], from the W3C).

Another possibility would have been to describe the interface and the behavior in a XML file. But, if we choose this approach, we cannot assure the interoperability between different Remote devices, and with other platforms.

What we need is a common language between different devices and the framework in order to exchange information between devices in a global entreprise system, which involves more than one device (mesh up of manufacturing tools). According to ontology paradigm, we define some concepts (named the vocabulary) and the relationship between these concepts (somehow the grammar). Ontologies are an answer to this problem since it is a normalized approach for the description of nature and composition of something. For example, a GUI is composed of buttons which have a localization, a level of use, but also which are related to an underlying function of the manufacturing system.

We established the ontology of devices that one could find in a laboratory. With such an ontology (see Figure 1), we are able to dress the complete GUI of a device without any link to the media which will be used to control it.

The vocabulary part of the ontology is common to all the devices. Upper the vocabulary, we have to described the functionalities of each device, which are obviously dependent of device type. The result is an OWL file per device grouping together the vocabulary and the "functionalities". With this approach, we have described in a semantic way very different devices such as a network analyzer and an antenna workbench and we are about to dress the OWL of an optic fiber stretcher.

The following figures (2 and 3) show very different manufacturing systems that are remote controlled thanks to the proposed software architecture.

B. Implementation

We use an Apache Web server to store the OWL file associated to each device. This file is downloaded by a Java Web Start application (a rich standalone client)

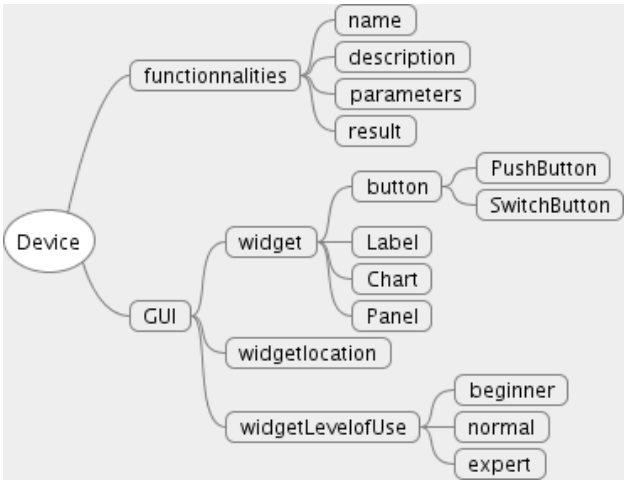

Figure 1. Part of the firm devices' ontology used for specializing distance interfaces.

[2] Ontology Web Language

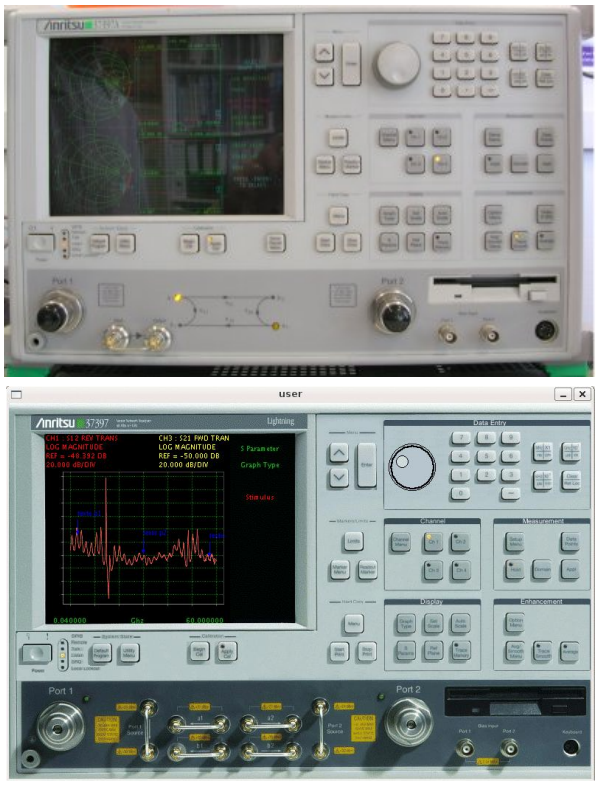

Figure 2. real interface of the network analyzer (above) and reconstructed remote interface tanks to OWL modelisation (bottom)

Figure 3. Manufacturing device (above), a laser powder technology, and zoom on its control system (Sinumerik 810D CNC form Siemens)

which parses it to build the distance interface of the real remote device. The result of this parsing step is the reconstruction of the graphical interface, and the association between widgets and device's functions. Then, an action over one widget (a button, a chart, a menu, ...) on the standalone client is delivered to an application server (for authentication, authorization and transactions) through a MOM[3] above. The application server relays the message to the device and back to others clients (to allow them what are the activities on the device). We use publish/subscribe paradigm [8] to deliver message to all actors of the system.

Mainly, the message between the client, the application server and the device are splitted in three types using ASK, ACK and ANS performatives :

- *ASK*, stand for "asking". This kind of message is sent when the user interacts with a widget. Then, this message is unicasted to the instrument with arguments describing the command (identifier, associated parameters, ...)
- *ACK*, stands for "acknowledgment". We need immediate reaction from the server side because commands performed on a device can last long (if an antenna needs to be moved for example). This message is multicasted to all the users allowing them to see that someone has asked this functionality or measurement.
- *ANS*, stands for "answering". Obviously, when the device has performed the actions corresponding to the request, it send the response to all the users (multicast message).

Upper this very simple protocol of message exchange, we use some normalized services to assure different tasks:

- we use JAAS[4] for authentication and authorization purpose. The framework verifies for each action if the user has the permission to do it. Since we try to be fully compliant to traditional Information System, the information about users credentials are stored within a LDAP directory (openLDAP is chosen as implementation).
- logging of the actions are made in a PostgreSQL database for two purposes : the post session evaluation by the teacher and the analysis of users' behavior.
- messages transportation is built thanks to a Java Messaging Service implementation : JORAM[5] , an ObjectWeb[6] open source Message Oriented Middleware.
- All the system is controlled by JOnAS[7], as we were looking for a J2EE certified application server.

With such an architecture, we are also able to propose collaboration over the same remote device. Indeed, the different messages coming from the different users are centralized through the MOM subsystem. Therefore, we put there an object in charge of the serialization of the different commands according to a collaboration policy. For example, the simplest collaboration policy can be :

[3] Message Oriented Middleware
[4] Java Authentication and Authorization Service
[5] Java Open and Reliable Asynchronous Messaging
[6] http://www.objectweb.org
[7] Java Open Application Server

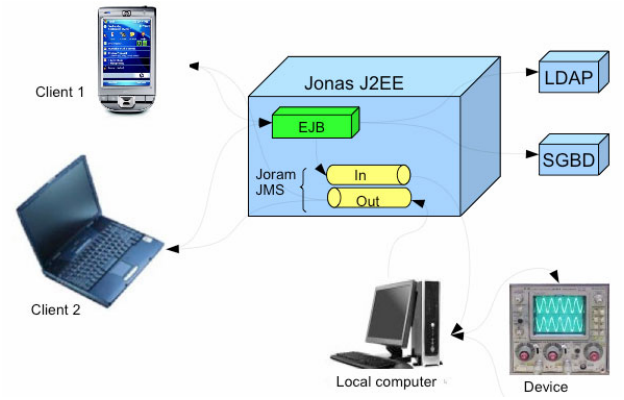

Figure 4. Online architecture we implemented.

« the user which is waiting for the longest delay will get the control of the device if he asked for through a command ». Once again, we propose the collaboration policy description through an ontology which describes the situation (users, roles, commands, delay,..) and a rule language to orchestrate the active user adjustment.

IV. DISTRIBUTED SECURITY

As we said in introduction, there is three axis of research to build a global solution for remote control of manufacturing systems. The two last points deal with security : security of the data and security of the information systems. This is clearly a major problem in most of the frameworks proposed in the literature, especially those dealing with solutions such as VNC (virtual network computer). Indeed, with this kind of solutions, the data are exchanged through clear connections allowing a man in the middle to get almost all the information he wants about your entreprise. The second drawback is you have the control not only of the remote device but on *the remote computer*, which can be considered as an unacceptable situation, considered by most of us as an authorized intrusion in Information System. Here, the framework is mainly on the server side allowing the centralization of data exchanges and the possibility to build crypted tunnels for the remote control and just one hole on the different firewall to access the main server. Moreover, the J2EE server asks an authentication server if the current client is allowed to use the remote device. Each command can be verified with this control, contributing to a very safe access to the device.

All these protocols have just one goal: to secure the access to the device and the data exchanges. Note that, the global architecture proposed in the previous section directly integrates the security aspects and we just have to build SSH tunnels and control the firewall to get an acceptable level of security.

But, this kind of scheme is correct if you trust the authentication server, and that the logged user is the man you think about. In fact, all the security tokens are given by this server (commonly a LDAP server). In an usual case, the client and the device are not from the same entity (for example, a firm proposes as a service the use of its devices to its clients inside supply chain. Another example is the access to your information system when you are away and therefore authenticated against another system). The probability that the client is already registered in the authentication server corresponding to the device is therefore very low. The worse solution is to create an anonymous account, or an account dedicated to the client, which is usually forgotten by the system administrator and remains in the identities repository. Moreover, anonymous identities do not allow a relevant accounting service. As a matter of fact, we think that a better solution lies in the fields of the identity federation. Indeed, if one have to wonder how to give access to some people to *one's* devices, there should have strong confidence in the distance user.

First and foremost, the milestone of a federation is about agreements between organizations about common standards in order to enable their interoperability. These standards concern namespaces, protocols, authentication contexts, identity information usage restrictions, cryptographic algorithms, etc. A federation also consists in partnerships to establish trust links. The whole make them confident enough to open their information system, and finally, to build an identity federation architecture. The business trust model should be designed at an organization level and not per service provider or per authority. So, in that case, it makes sense to have what is called a Trust Gateway (TG) for each organization to manage the business trust model. In a federation context, entities linked by a business trust model form what is often called a Circle of Trust (CoT).

In a CoT, one can use the security tokens from one authentication server in order to use the services proposed by the other system, and for example open the facility to use remote controlled manufacturing systems. The first thing to do is to determine if the remote parties feel confident enough to trust each other. If the answer is positive an organization can trust the other one to establish the identity of their users and provide signed information about them. The basics of identity federation is the establishment of a trust architecture between partners and the implementation of protocols allowing to retrieve signed information. The main expected functionalities are identification of partners' members, establishment of user identity, and being able to retrieve information about them.

The stake of identity federation between Information Systems is the interoperability through normalized protocols. The objective is not to build a metaserver which collects and synchronizes information from slave servers, but to build a decentralized architecture built on a consensus to safely exchange identity information. The federation can be based on different protocols, leading to different solutions. At this time, the main architectures, such as universities or e-government, are SAML-based [1] through Liberty Alliance [21]. We have contributed to SAML implementation in order to propose a complete solution of identity federation named *FederID* [4]. This solution is based on different tools: a reverse proxy (lemonLDAP), an (or multiple) identity provider (Authentic) and an attribute provider (InterLDAP). The figure 5 summarizes the different security information exchanges through Web Services in three Circles of Trust. With this kind of structure, a client can use a device belonging to another Information System, provided that both information systems are in the same CoT.

Current identity federation specifications and implementations consist in Web services oriented middleware

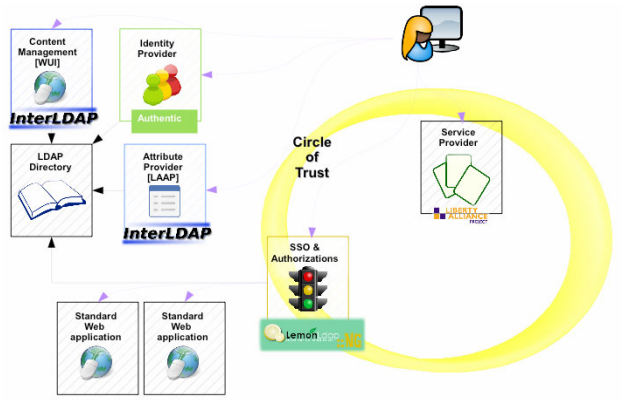

Figure 5. Principle of identity federation in the FEDERID Project : the different providers

used as a security layer by third Web applications and Web services oriented architectures, therefore mainly based on HTTP and XML. Serialization via XML, and message transport through HTTP, contribute to the proposed architecture of FEDERID. Nevertheless, it still misses standard for security schemes and identity attributes namespaces. OASIS SAML2, Liberty Alliance ID-WSF, Cardspace and WS-Federation partly address some of these requirements; but for now, no standard predominates. Only the SAML assertions XML application, as a serialization of identity information, seems to become a standard that can be used to allow uses in an industrial context such as the security part of the remote control of manufacturing systems.

V. CONCLUSIONS

In this paper, we have tried to address all the parts which are involved in the remote control for manufacturing systems and maintenance:

- the independence of the framework to the device in order to put more and more devices online without reinventing the wheel each time,
- the exchange of the required security tokens and the privacy of entreprise data.

For each of these parts, we have shown how the problem can be solved and we have proposed and implemented a solution, giving us the opportunity to propose a global framework for remote control of devices [9] which is applied to industrial context.

Obviously, there is still a lot of work to be done in order to propose a complete set of remote devices in such contexts. Among the principal tasks, we plan to address quickly:

- the evaluation of the framework according to its usability through adirect investigation of users,
- how to confirm the genericity of the proposed framework through the proposalof new devices.

ACKNOWLEDGMENTS

This work is granted thanks to the General Council of Loire Department, France and by the French National Agency of Research (FEDERID project).

REFERENCES

[1] Security assertion markup language (saml) v2.0. Technical report, OASIS, http://www.oasis-open.org/specs/index.php, 2006.

[2] H. Abdel-Wahab, K. Maly, A. Youssef, E. Stoica, M. Overstreet, K. Wild, and A. Gupta. The software architecture and interprocess communications of IRI: an Internet-based interactive distance learning system. In I. C. Society, editor, *Proceedings of the 5th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'96)*, page 4, 1996.

[3] J. R. Anderson, J. Fincham, and S. Douglass:. The role of examples and rules in the acquisition of a cognitive skill. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 23:932–945, 1997. (doi:10.1037/0278-7393.23.4.932)

[4] M. Ates, C. Gravier, J. Lardon, J. Fayolle, and B. Sauviac. Interoperability between heterogeneous federation architectures : illustration with saml and ws federation. In *SITIS-Septis'07 IEEE International Conference On Signal-Image Technology and Internet based systems, Workshop on security and privacy in telecommunication and information system*, December 2007.

[5] B. Bayard, B. Sauviac, J. Fayolle, B. Allard, and G. Noyel. Projet webanalyzer internet et l'instrumentation à distance. In *TICE 2002, Technologies de l'information et de la communication dans l'Enseignement Supérieur et l'Entreprise*, pages 415–416, Novembre 2002.

[6] A. R. S. Castellanos, L. H. Santana, E. Rubio, I. S. Ching, and R. A. Santonja. Virtual and remote laboratory for robot manipulator control study. *The International Journal of Engineering Education*, 22(4):702–710, 2006.

[7] Estrem, W., An evaluation framework for deploying web services in the next generation manufacturing enterprise. Robotics and Computer-Integrated Manufacturing, 19(6), 509–519, 2003

[8] K. Geihs. Middleware challenges ahead. *IEEE Computer*, 34:24–31, 2001. (doi:10.1016/S0736-5845(03)00061-9)

[9] C. Gravier and J. Fayolle. Web site of the einst project. Technical report, Istase, http://diom.istase.fr/satin/einst, 2007.

[10] C. Gravier, J. Fayolle, B. Bayard, M. Ates, and J. Lardon. State of the art about remote laboratories paradigms - foundations of the ongoing mutations. *iJOE : International Journal of Online Engineering*, 4(1):19–25, February 2008.

[11] T. Gruber. Toward principles for the design of ontologies used for knowledge sharing. *Elsevier Science Ltd.*, 43:907–928, 1993.

[12] S. Guss. Interface metaphors and web-based learning. *Lecture Notes in Computer Science*, 2783:168–179, 2003.

[13] Hao, Q., Shen, W., and Wang, L., Towards a cooperative distributed manufacturing management framework. Computers in Industry, 56(1), 71–84, 2005 (doi:10.1016/j.compind.2004.08.010)

[14] Jiang, P. and Fukuda, S. Telerp - an internet web-based solution for remote rapid prototyping service and maintenance. International Journal of Computer Integrated Manufacturing, 14(1), 83–94, 2001 (doi:10.1080/09511920150214929)

[15] Lee, J. E-manufacturing-fundamental, tools, and transformation. Robotics and Computer Integrated Manufacturing, 19(6), 501–507, 2003. (doi:10.1016/S0736-5845(03)00060-7)

[16] Lee, J., Ni, J., Djurdjanovic, D., Qiu, H., and Liao, H. Intelligent prognostics tools and e-maintenance. Computers in Industry E-maintenance Special Issue, 57(6), 476–489, 2006.

[17] Lin, H., Harding, J., and Choudhary, A. The universal knowledge moderator for globally distributed and collaborative e-manufacturing. In INDIN 2008, 6th IEEE International Conference on Industrial Informatics, 1227–1231. 2008

[18] Lujiong, W., Aiping, L., and Liyun, X. A security model for networked manufacturing system. In International Conference on Computational Intel ligence and Security,745–749, 2007

[19] J. McCarhty and P. Wright. Putting felt-life at the centre of human-computer interaction. *Proceedings of In Reflective HCI Workshop*, 2004.

[20] Molina, A. and Santaella, A.R. Achieving e-manufacturing: multihead control and web technology for the implementation of a manufacturing execution system. Journal of Intel ligent Manufacturing, 17(6), 715–724, 2006 (doi:10.1007/s10845-006-0040-2)

[21] B. Pfitzmann. Privacy in enterprise identity federation: Policies for liberty single sign on. *Lecture notes in computer science Privacy Enhancing Technologies*, pages 189–204, 2003.

[22] Tan, J., Wen, H.J., and Gyires, T. M-commerce security: the impact of wireless application protocol (wap) security services on e-

business and e-health solutions. International Journal of Mobile Communications, 1(4), 409–424, 2003 (doi:10.1504/IJMC2003.003994)

[23] Wang, L., Orban, P., Cunningham, A., and Lang, S. Remote real-time cnc machining for web-based manufacturing. Robotics and Computer-Integrated Manufacturing, 20(6), 563–571, 2004 (doi:10.1016/j.rcim.2004.07.007)

AUTHORS

J. Fayolle, C. Gravier, M. Ates are with the Laboratoire DIOM, TELECOM Saint-Etienne, ecole associée de l'Institut TELECOM, Université de Saint-Etienne, and Université de Lyon, France.

Submitted 20 July 2009. Published as resubmitted by the authors on 8 November 2009.