Unified enterprise modelling language-based interoperability for collaborative access control framework in critical infrastructures

Amine Baina*

Laboratoire de Systèmes de Télécoms, Réseaux et Services (STRS),
Institut National des Postes et Télécommunications (INPT),
2, Avenue Allal El Fassi, Rabat, Morocco
Email: baina@inpt.ac.ma
*Corresponding author

Khalid Benali

CNRS, Inria, LORIA,
Université de Lorraine,
F-54000 Nancy, France
Email: Khalid.Benali@loria.fr

Mostafa Bellafkih and Nawal Ait Aali

Laboratoire de Systèmes de Télécoms, Réseaux et Services (STRS),
Institut National des Postes et Télécommunications (INPT),
2, Avenue Allal El Fassi, Rabat, Morocco
Email: mbellafkih@yahoo.com
Email: aitaali@inpt.ac.ma

Abstract: Due to physical and logical vulnerabilities, a critical infrastructure (CI) can encounter failures of various degrees of severity, and since there are many interdependencies between CIs, simple failures can have dramatic consequences on the whole infrastructure. In this paper, we mainly focus on malicious threats that might affect the communication and information systems (the critical information infrastructure, or CII) dedicated to critical infrastructures. We define a new collaborative access control framework called PolyOrBAC, to address the security problems that are specific of CIIs. This approach offers each organisation taking part in the CII the capacity of collaborating with the other ones, while maintaining a control on its resources and on its internal security policy. The approach is demonstrated on a practical scenario, based on real emergency actions in an electric power grid infrastructure.

Keywords: critical infrastructure; critical information infrastructure; CII; security; access control policies and models; collaboration; interoperability; virtual organisations; collaborative access control; electrical grid; unified enterprise modelling language; UEML.

Reference to this paper should be made as follows: Baina, A., Benali, K., Bellafkih, M. and Aali, N.A. (2020) 'Unified enterprise modelling language-based interoperability for collaborative access control framework in critical infrastructures', *Int. J. Networking and Virtual Organisations*, Vol. 22, No. 1, pp.75–100.

Biographical notes: Amine Baina is an Assistant Professor at the National Institute of Posts and Telecommunications Rabat, Morocco, since 2010. He had his PhD in Computer Science in Access Control for Critical Infrastructures in 2009 from the Laboratory of Systems Analysis and Architecture in Toulouse. He had his Computer Engineer's degree from the National Engineering School of Bourges, France in 2005.

Khalid Benali received his PhD in Computer Science from the Nancy 1 University, France in 1989 and Habilitation à Diriger les Recherches (HDR) from the Nancy 2 University, France in 2004. He is an Associate Professor, HDR at the Lorraine University and researcher within COAST team of LORIA (CNRS-Inria-Lorraine University). His lectures are mainly in the area of distributed systems and object oriented analysis and design for postgraduates and his research interests are in the area of distributed and cooperative systems, and integration/interoperability of virtual enterprises.

Mostafa Bellafkih is a Full Professor at the National Institute of Posts and Telecommunications Rabat, Morocco with a Doctorate in Applied Sciences (Networks and Computer Systems) from the Mohammadia School of Engineers, University Mohamed V Rabat in 2001. He achieved his Doctoral thesis in computer sciences in 1994 from the University Pierre-et-Marie-Curie (Paris 6).

Nawal Ait Aali completed her Engineering studies in Telecommunication Systems and Networks at the National School of Applied Sciences from 2007 to 2012. Currently, she is preparing her PhD in Computer Science at the National Institute of Posts and Telecommunications (INPT) at Rabat, Morocco. She works in her thesis on the trust management in the collaborative systems for critical information infrastructure protection.

1 Introduction and background

Critical infrastructures (CI) are logical/physical facilities of essential importance for public welfare, and their failure or disruption could potentially have a dramatic impact on economic and social welfare of a nation, a society, or an economy. The most significant examples of CI are those dedicated to electricity generation, transport and distribution (i.e., the electric power grid), telecommunications, supply services (energy, food, fuel, water, and gas), transportations systems (roads, railways, and airports), financial services (banks, stock exchange, and insurances), etc. due to interdependencies between various infrastructures, cascading failures[1] and escalating failures[2] are not unlikely (Rinaldi et al., 2001; Laprie et al., 2007). A simple failure can result in an important power outage like the North America blackout occurred on 14 August 2003 (Amin, 2003). One of the immediate causes of this large blackout, which caused 6 billion dollars of losses according to the US Department of Energy, was a failure of the monitoring software, which prevented confining an electrical line incident, before its propagation across the electrical power grid. Such failure scenarios might occur as a result of accidental faults as well as of malicious threats (intrusions, worm propagation, denial of service attacks, etc.). These CI are controlled by information and communication technology (ICT) systems, called critical information infrastructure (CII). These CII involve vulnerable information technologies, which can be targeted and compromised by malicious attackers. Security of CII is then becoming an important topic of many research studies. On the other hand, to deal with the changing needs of the market, the structure of the CII must be flexible and extensible (co-operation with new organisations, possibly on new geographical areas). Consequently, the CII must consist of an open, and distributed system, to allow the organisations composing it to collaborate within the CII and provide resources accessible by internal and external users.

With the opening and the deregulation of markets, some of these organisations can be in competition, while collaborating. It is the case in Europe in particular, where regional, national or multinational companies are in competition but must cooperate to produce, transport and distribute electric power. This induces an essential need for access control to manage different accesses from an organisation to the other.

Many organisations are currently forced to collaborate with others in renewing their products and processes to stay competitive, to enter new or to retain their current markets, or to get easy access to new knowledge. Management of collaboration between two or more organisations is, however, still not well understood, given that about half of the collaborative endeavours fail. A methodology to support management of collaboration is still lacking. To build such a methodology, knowledge is needed on the process of collaboration. Much research has been devoted, however, to understanding the relationships between initial conditions and outcomes of a collaboration initiative. The results of this research are sometimes contradicting or not very well comparable because of differences in conceptualisation or ignorance of moderating factors. Moreover, a good design of initial conditions is necessary, but not sufficient. Conditions change during the process of collaboration. We need knowledge on the dynamics of the collaboration process to understand why and how conditions change and how they can be influenced. In this paper an approach will be presented that can support the gradual building of knowledge on the process of collaboration. The approach, which resulted from the Esprit IV project 23286 fast reactive extended enterprise (FREE), can be viewed as a first step towards building a methodology to support management of collaboration. The concept of infrastructures for collaboration will be introduced stressing the integral nature of management of collaboration. Authors of research paper (Wognum and Faber, 2002) introduce the concept of infrastructures for collaboration in virtual organisations (VOs).

Another form of collaborative organisation is collaborative networked organisation (CNO). The authors in Noran (2006) refine a meta-methodology for collaborative networked organisations. Presently, there is a great need for methodologies and reference models to assist and guide the creation and operation of various types of enterprises, including CNO. The efforts to fulfil this need can be significantly assisted by a meta-methodology integrating current and future CNO creation and operation knowledge. Their work presents a milestone in an iterative and reflective action research aiming to demonstrate the feasibility of such a meta-methodology. The study describes a field experiment combined with a case study and subsequent reflections leading to the refinement and extension of the proposed meta-methodology. In the field of collaborative manufacturing, the authors in Shamsuzzoha and Helo (2015) present a virtual business process management system. Business collaboration in the form of virtual factory is nowadays considering as one of the critical factor in the manufacturing community, mostly within small and medium size enterprises (SMEs). In such an environment, it is very important to deal with accompanying process details within virtual factory environment. Their research articulates fundamental concepts of the virtual business network in the form of plug-and-play virtual factory, where both intra and inter-organisational processes are defined for the purpose to execute the virtual collaboration successfully. Different phases of virtual factory and its associated process steps are defined with necessary annotations. The work presented in Walker (2006) presents the VO as a new organisational form. The VO is conceptualised by many researchers as a new organisational form. It represents a radical shift from the traditional organisation and makes new ways of organising possible. Such expectations are explored, and the meanings and interpretations of the VO for its designers and virtual workers are investigated in a project that seeks to develop a virtual (reality) organisation. This research involved longitudinal participant-observation with the VO design team and interviews with organisational members. Contrary to indications in the literature, this research found that the VO in this instance is predominantly conceived by designers and users as an extension of the existing organisation, rather than representing radical organisational change.

In research paper (Yen et al., 2002), the authors present a strategic approach to become a VO. It is an emerging organisational concept that brings new managerial strategies and requires a feasible and flexible information infrastructure. This paper provides a strategic discussion on how to become a VO and focuses on its features, models and applications, as well as managerial and technical requirements. The authors in present (Verginadis et al., 2011) examines how ontologies can be employed by a system of services for delivering interoperability to enterprises, independent of particular IT deployments. In order to support interoperability service utilities in VOs, the paper presents a top-level ontology for collaborative networked organisations (code named OCEAN). The OCEAN ontology is designed as a lightweight top-level ontology that provides a common terminological reference in terms of VOs. The paper also demonstrates the use of practical tools for achieving consensus of the shared conceptualisation of a VO, among participants, while it outlines a service-oriented architecture (SOA) for supporting VO knowledge-based collaborations using OCEAN. The authors demonstrate how that usage enables shared understanding in knowledge-intensive collaborations, as well as how it facilitates interoperability of applications that provide collaboration services, presenting concrete examples from the pharmaceutical industry. In a similar way, the study (Preis and Seitz, 2012) addresses challenges, which appear when heterogeneous data warehouses are integrated. Such a scenario especially shows up in the environment of VOs. The involved companies, of the before named constellation, need to combine their business data to attain ‘one single version of truth’ for decisions beyond organisational borders. The occurring issues are depicted and analysed from an exemplary and theoretical point of view. Not only weaknesses, but also reasons for those shortcomings are analysed. The study presents a working definition of the term ‘VO’ and the link and interdependence to information technology is offered. The study also discusses schema and mapping conflicts, organisational deficits, which are probably a facilitator for those problems. Moreover, path breaking decisions within a data warehouse integration project are visualised, to provide decision makers with some rough reference points. The paper (Preis and Seitz,

2012) is completed by a view on the human component and an outlook on in-memory computing.

Another need for VO is dynamic composition and decomposition. In work (Karakostas, 2014), the authors present cloud architecture for dynamic VOs in transport logistics. Their work proposes a cloud-based data sharing architecture for dynamic VOs in the domain of transport logistics. Such VOs are described as dynamic because its members can join and leave on demand, reflecting the behaviour of physical transport chains. Members of the VO implement a community type cloud by sharing amongst them data resources over a cloud fabric. Data about the status and activities of the transportation chain are replicated intelligently across the participating nodes. The data cloud architecture proposed in this paper ensures that transport chain data are always available on demand to those that require them, while minimising unnecessary exposure of data and thus security risks. The approach is illustrated with a case study of a multimodal transport logistics chain VO. Authors (Alawamleh and Popplewell, 2012a) of study: analyse VO risk sources through an analytical network process (ANP) approach, the SMEs have to collaborate with other enterprises in a VO forms to cope with an increasingly dynamic and competitive environment. Despite the increased interest in the area of collaboration information is still lacking about the risk sources of VO. This paper aims to reinforce the proposal for an integrated methodology to classify, manage and assess network level risk sources in VO and discusses the advantages of AHP/ANP over the other multi-criteria decision making (MCDM) methods before discussing the analytical hierarchy process (AHP) and the ANP methods and the advantages of ANP over the AHP. This will be followed by illustrations of how ANP can be used to assess VO risk sources as part of the framework to support the final decision of VO collaboration. ANP will be used to set up a panel of weights of risk sources to define which risks are more serious. Overall, insights from the research and the process suggested in this research will aid SMEs in making a less risky decision (Alawamleh and Popplewell, 2012a). In another study (Alawamleh and Popplewell, 2012b), the authors discusses the risk in VO, environment within which SMEs have to function in the 21st century is one that is increasingly competitive and dynamic and therefore, simply to cope in such a situation, SMEs have to seek for a number of methods to employ and one of these is to group together within a VO. It is, however, not easy to become part of a VO and there are risks to be dealt with throughout the whole process from the initial formation of such a group through to the point where it dissolves. In order that the challenges can be met successfully, it is important that enterprises should be helped to both recognise the risks and then surmount them. Based on case study, this study (Alawamleh and Popplewell, 2012b) aims to develop a deeper understanding of the main constructs of risk sources in VOs, especially their dependencies and perceptions. Another interesting work (Correia Alves and Rabelo, 2013) describes a KPI model for logistics partners' search and suggestion to create VOs, it presents an exploratory and qualitative work of a novel model for the selection of the most adequate logistics providers to compose VOs. It includes a performance measurement model and a supporting methodology that considers the intrinsic dynamics, autonomy and temporality of VOs, involving both intra and inter-organisational strategic indicators. The model is flexible in terms of both allowing performance indicator weight relaxation and being adapted according to the organisation's governance model. A software prototype was developed and interviews with specialists were carried out to evaluate the model.

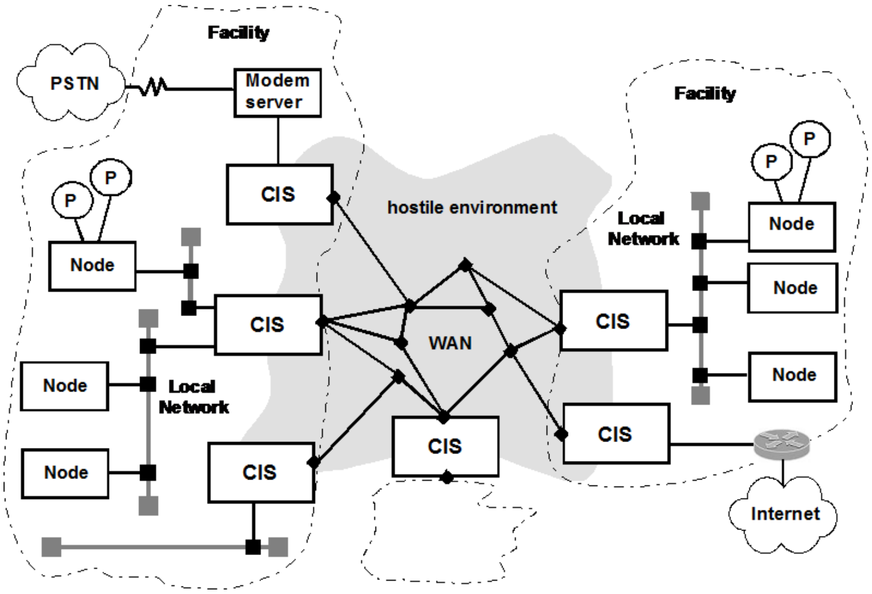
In another study (Petersen, 2007), the authors present an analysis using case studies for virtual enterprise (VE) formation and partner selection. A VE can be described as an organisational form that emerges when individual entities form a team of partners to achieve a specific goal. The ability to assemble the best team is critical to the success of the VE and this imposes strong demands on its formation. In this paper, the authors present an agent-based model of a VE, where the partners of a VE are represented by software agents. They show how this model can support the different processes that are used in industry for selecting the partners. Industrial case studies have been used to illustrate the different partner selection processes that are used in industry. The selection processes are analysed using agent interaction protocols (AIP) to describe the interactions that take place between the different entities (Petersen, 2007).

In this paper, mainly based on Baina et al. (2009) and Panetto et al. (2004), we focus on security problems related to access control, collaboration, and interoperability between the organisations and the systems composing the CII. And we show how PolyOrBAC (Kalam et al., 2007; Baïna et al., 2009), a security framework based on the OrBAC access control model (Kalam et al., 2003; Cuppens et al., 2005) and web services (WS) technology, can be adapted to cope with CII security needs and how the unified enterprise modelling language (UEML) model (Panetto et al., 2004) can be instantiated with the electrical grid scenario studied in the PolyOrBAC framework. The remainder of this paper is organised as follows: Section 2 presents the general architecture of a CII. Section 3 presents a sketch of our proposal and the needed background information, including the OrBAC model and the WS technology, and then a typical execution scenario. Section 4 discusses the use of UEML (Panetto, 2004) for interoperability issues management. Section 5 shows how PolyOrBAC can be applied to the electrical power grid CII and how the UEML model can be instantiated with the electrical grid scenario studied in PolyOrBAC framework, and finally Section 6 draws up the conclusions and proposes possible extensions of this work. The following section is based on (Baina et al., 2009).

2 The CRUTIAL infrastructure

In order to easily understand how to apply PolyOrBAC in the context of CII, we describe in this section, the general architecture (cf. Figure 1) proposed by the European project CRUTIAL (Dondossola et al., 2006) to ensure the protection of interconnected CIs, in particular those used in the context of electrical power grids, against malicious as well as accidental threats. The CII architecture can be seen as a WAN of LANs inter-connected by CRUTIAL information switch (CIS). Each LAN, is composed of logical/physical systems, has its own applications and access control policy, and proposes its services to other systems. Each LAN belongs to organisations involving different actors and stakeholders [e.g., power generation companies, power plants, substations, energy authorities, external maintenance service providers, and transmission and distribution system operators (DSO)]. More than one LAN can be connected by the same CIS if they are part of the same organisation and located in the same area. In this case, each LAN is dedicated to a component (e.g., substation), in order to manage a different access control policy for each component. Considering the CRUTIAL architecture described above as an example, since all organisations of the CII are interconnected by CIS, and in order to provide a controlled cooperation adapted to the CII, each CIS must contain mechanisms to enforce the local security policy of its organisation, collaboration mechanisms thanks to WS should also be implemented (so that the various organisations can offer services and collaborate with each other). These policies and mechanisms must allow the authorised accesses to the resources and prevent the unauthorised accesses (accidental or malicious ones). The following section is based on (Baina et al., 2009).

Figure 1 General architecture of a CII



Source: Baïna et al. (2009)

3 PolyOrBAC framework for access control and collaboration in CIIs

There are some interesting approaches using the XACML language to manage access control in distributed and decentralised systems (Lorch et al., 2003) XACML is useful for specifying policies in distributed environments. The standard format works well in tying together heterogeneous systems, its definition in XML, and availability of open source projects has already drawn support from diverse applications. However XACML's flexibility and expressiveness comes at the cost of complexity and verbosity. It is hard to work directly with the language or policy files. Tools are underway, but until there is widespread availability, it will be hard for average users to work with any XACML-based system. As an alternative, we use the OrBAC access control model, which is described later, to develop our approach. Our goal is to guarantee access control for each different component of the CII, and guarantee collaboration between these components. Globally, there are two approaches to fulfil this objective. The first consists in imposing a global and centralised security policy for all the concerned organisations. This approach is not appropriate for a CII, because of its dynamic character (organisations should be able to join or leave the CII without disturbing the whole CII architecture), but also because organisations are mutually suspicious and do not trust each other's: each organisation, with specific features, specific functioning rules and security policies, wants to keep its autonomy, and refuse to open its information system to competitors or to change its security policy.

The need for trust has been well depicted in work (Khan, 2012), which presents the role of trust and relationships in geographically distributed teams: exploratory study on development sector. Interviewed teams were surrounded by ground realities of their work locations, which included technology limitations, uncertainties and human constraints, which tend to obstruct development of trust and relationships. The needs for developing trust and relationships identified during interviews were personal conduct characteristics of team members, like confidence, competence, reliability, interpersonal relationship, quality output, responsibility and commitment. Trust emerged as the core factor encompassing all relationships, among team members or between leader and members. The study revealed that trust is a precursor to relationships. Geographically distributed teams work within cognitive trust, where its members desire affective trust from the leader. Trust is not only a product of, but also a pre-requisite for optimal technology usage. Trust is not formally evaluated but is manifested in the quality of outcomes. Another work, (Daassi et al., 2006) presents an empirical investigation of trust's impact on collective awareness development in virtual teams. This study investigates the relationship between trust and collective awareness levels over time. The study also examines the multi-dimensionality of both trust and collective awareness in virtual teams. Hence, we adopt a longitudinal study to provide a preliminary step towards understanding the dynamic nature of trust and collective awareness in virtual teams. The results of this study show that (Bhat et al., 2017) both trust and collective awareness levels increase over time; (Mattos and Laurindo, 2015) during the project, task processes are more important than socio-emotional processes; and (Preis and Seitz, 2012) higher (vs. lower) trust levels are associated with higher (vs. lower) collective awareness levels. The authors of study (Wu and Li, 2009) discuss inter-organisational trust in B2B commerce. Research studying trust in business-to-business (B2B) relationships is only burgeoning compared to its B2C counterpart. The authors find an increase in studies on trust in B2B and inter-organisational systems (IOSs). They group some commonalities found into three types of trust: relationship, technology and third-party and fit them in a general framework. They also identify four patterns with which researchers operationalise and test B2B trust and evaluate the empirical support for each. The authors of study (Ignatiadis et al., 2006) discuss how to promote trust in B2B VOs through business and technological infrastructures. The purpose of their work is to propose ways to increase the level of trust in online B2B communities, through the use of business and technological schemes. From the business point of view, two mechanisms are proposed:

1 The use of service level agreements, special forms of contracts popular in the provision of IT services industry, which can be introduced to cover all legal and non-legal requirements of online trading.

2 The establishment of support centres, which can act as intermediaries between companies in case of dispute, and which can guarantee the trustworthiness of the companies involved in e-commerce.

From the technological point of view, the use of a peer-to-peer approach in B2B e-commerce is discussed. From an empirical perspective, the work within the framework of the European Union co-funded research project 'LAURA' is presented.

The second approach, on which our access control framework PolyOrBAC is based, consists in managing collaboration between the various organisations of the CII while keeping autonomy of each one. PolyOrBAC (Kalam et al., 2007) is based on two principal components: the OrBAC access control model, and the WS technology. PolyOrBAC makes it possible to ensure the access control and the security of the CII by specifying local access control policies with OrBAC (for each organisation composing the CII), and managing collaboration rules between these various organisations through the use of WS. Thus, PolyOrBAC ensures interoperability, collaboration and the secure sharing of information between the various components, actors or organisations of the CII, by the use of WS technology. In this section, we first present the needed background, and then we will show how OrBAC can be coupled with WS, leading to the PolyOrBAC framework.

3.1 OrBAC access control policies

The OrBAC (Kalam et al., 2003) model is an extension of RBAC (Sandhu et al., 1996; Ferraiolo et al., 2001). It enables a structured and abstracted expression of the policy: Subjects are abstracted in roles (as in RBAC), objects (Brose, 1999; Bell and LaPadula, 1976) in views (as in VBAC, Brose, 1999; Fink et al., 2003) and actions (Bell and LaPadula, 1976) in activities (as in TBAC, Sainan, 2010). Also, the specification of the security policy is completely separated from its implementation, so as to easily manage complexity. In OrBAC, an organisation is a structured group of active entities, in which subjects play specific roles. An activity is a group of one or more actions, a view is a group of one or more objects, and a context is defined as a specific situation that conditions the validity of a rule. The role entity is used to structure the link between the subjects and the organisations. In the same way, the objects that satisfy a common property are abstracted as views, and activities are used to abstract actions. OrBAC rules can express positive/negative authorisations (permissions/interdictions), and obligations. Security rules have all the following form: permission (org; r; v; a; c), prohibition (org; r; v; a; c), or obligation (org; r; v; a; c). Such a rule means that in context ‘c’, organisation ‘org’ grants role ‘r’ the permission (or the prohibition, or the obligation) to perform activity ‘a’ on view ‘v’. OrBAC considers two different levels for the security policy: the abstract level and the concrete level. At the abstract level, the security administrator defines security rules through abstract entities (roles, activities, views) without worrying about how each organisation implements these entities. At the concrete level, when a user requests an access, concrete authorisations are granted (or not) to him according to the concerned rules, the organisation, the played role, the instantiated view/activity, and the current parameters. The derivation of permissions (i.e., instantiation of security rules) can be formally expressed as follows:

$\forall$ org $\in$ Organisations, $\forall$ s $\in$ Subjects, $\forall$ activ $\in$ Activities, $\forall$o $\in$

Objects, $\forall$ r $\in$ Roles, $\forall$ a $\in$ Actions, $\forall$ v $\in$ View, $\forall$ c $\in$ Contexts,

Permission (org, r, v, activ, c) $\wedge$

Empower (org, s, r) $\wedge$

Consider (org, a, activ) $\wedge$

Use (org, o, v) $\wedge$

Hold (org, s, a, o, c)

$\Rightarrow$ Is permitted(s, a, o).

Which means, If a security rule specifies that in ‘org’, role ‘r’ can carry out the activity ‘activ’ on the view ‘v’ when the context ‘c’ is True, and in ‘org’, ‘r’ is assigned to subject ‘s’, and in ‘org’, action ‘a’ is a part of activity ‘activ’, and in ‘org’ object ‘o’ is part of view ‘v’, and the context ‘c’ is true for the triple (org, s, a, o). Then subject ‘s’ is allowed to carry out action ‘a’ on object ‘o’.

3.2 OrBAC limits

OrBAC has attracted a growing scientific community, and many research tracks are being conducted based on it. Also, it is suitable for real world environments and can specify complex and flexible security policies that match IT systems reality. Moreover, the specification, management and update of security policies are easily carried out, thanks to its user-friendliness. In the context of the CII, we must not only specify the security requirements/rules for each organisation/subsystem of the CII, but also manage collaboration between these organisations and enforce (into each CIS) the different security policies. OrBAC can handle the first point, while making it possible to specify complex and flexible security policies for each organisation, but it does not deal with the second problem. In fact, it is not possible to specify the rules which imply several independent organisations belonging to a collaborative system in the same OrBAC policy. Moreover, it is impossible to associate permissions to users belonging to other partner-organisations (or to sub-organisations). Consequently, if OrBAC provides a framework to express the security policies of each organisation, it does not meet the needs for distribution, collaboration and interoperability between different organisations. The WS technology provides some mechanisms – in particular for collaboration – which are very relevant for our work. The next subsection presents this technology.

3.3 WS for interoperability and collaboration

WS are a set of technologies that provide platform-independent protocols and standards used for exchanging heterogeneous interoperable data services. Software applications from various platforms written in various programming languages and running on various platforms can use WS to exchange data over computer networks in a manner similar to inter-process communication on a single computer. They use well-known and open standards and protocols such as XML (W3C, XML, 2004), SOAP (W3C, SOAP, 2003), WSDL (W3C WSDL, 2006) and UDDI (OASIS, 2005) and can be used easily with the current Web interfaces. Being based on the HTTP protocol, WS can cross firewalls, without changing the pre-established security requirements. Moreover, the execution of a WS does not require necessarily huge resources (memory, power and CPU time), and a small quantity of code is sufficient for its implementation. Finally, it is easy to couple WS with the operation of OrBAC. Equations should be punctuated in the same way as ordinary text but with a small space before the end punctuation mark.

In a similar study (Namin et al., 2006); authors implement enterprise collaboration using WS and software agents. Global competition has forced manufacturing enterprises to collaborate towards fulfilling market demands and satisfying customers. A major challenge in implementing enterprise collaboration is on the integration of heterogeneous hardware and software platforms. This paper (Namin et al., 2006) proposes to implement enterprise collaborations by employing WS and software agents. It presents a multi-layer architecture for enterprises' software infrastructure capable of accomplishing the necessary functionalities in typical collaborations such as resource discovery, workflow coordination, request analyses, tasks assignment and monitoring. In addition, the authors propose an agent-based multi-layer structure for service discovery to improve the functionality and efficiency of resource discovery.

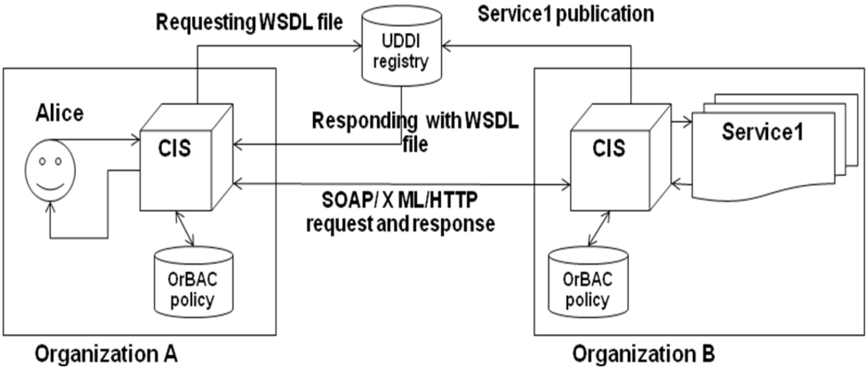
The study depicted in King and Kawash (2011), presents a real-time XML protocol for bridging virtual communities. Virtual communities play an increasingly important and prevalent role in our daily lives. However, these communities are often closed relative to each other, forming independent islands of communities. Yet, this independence is artificially imposed on such communities by closed support software or policies since the purposes or member-bases of these communities often overlap. The objective of that paper is to bridge these virtual communities, allowing them to seamlessly and securely mesh in spite of their differing implementations and autonomous policies (King and Kawash, 2011).

3.4 PolyOrBAC architecture

PolyOrBAC uses OrBAC to specify local access control policies (for each organisation) as well as collaboration rules implying several organisations. On the other hand, WS are used to enforce collaboration. In fact, each component (organisation/subsystem) of the CII could have its own security objectives and should be able to cooperate with the other components. Each organisation contains its own resources, services, applications, with its own objectives, operation and security rules, and policy. Each organisation could specify its security policy according to OrBAC. In the example of Figure 2, organisation 'B' offers the WS 'Service1' and Alice from organisation 'A' wishes to invoke 'Service1' from organisation 'B'. Firstly, during the publication step, each organisation (e.g., 'B') determines which resources/services it proposes to external partners. WS are developed on the organisation's application servers, they are defined in the organisation's OrBAC security policy and they are referenced in the organisation's CIS to be accessible to external users. Secondly, at the discovery step, when a user (e.g., Alice) of organisation 'A' wants to use 'Service1', org 'A' contacts the UDDI WS registry to search for 'Service1' (published beforehand by the offering org 'B'), then 'A' receives the WSDL file containing the description of 'Service1' as well as the URL of the site (i.e., org 'B') that hosts 'Service1'. Thirdly, at the negotiation step, organisations 'A' and 'B' are authenticated mutually in order to prove their identities, then they negotiate and come to an agreement, they establish a contract and jointly define security rules about the access to 'Service1'. These rules and contracts are registered – according to the OrBAC format – in each CIS database containing the security policy.

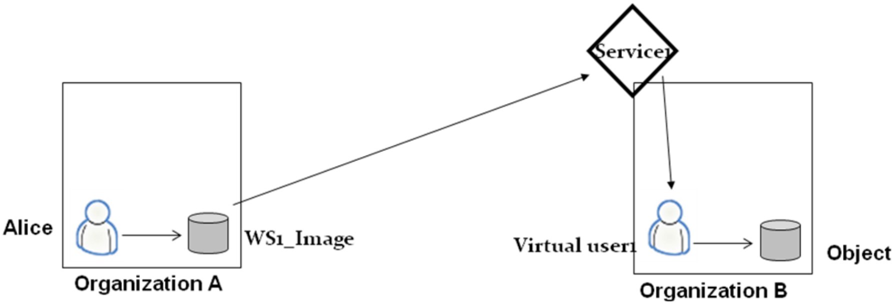
As explained in Figure 3; organisation 'A' wants to avoid using the UDDI registry every time it invokes 'Service1', and it wants to have a local representation of a remote requested 'Service1' in order to manage the access control policy locally, so 'A' locally creates 'ws-image1' accessed by only authorised users of 'A'. Organisation 'B' wants to have a local representation of the remote organisation 'A' that requests 'Service1', in order to virtualise the distant access from 'A' and to manage it like a local access in 'B', so 'B' locally creates 'virtual-user1' playing an OrBAC role enabling to perform the activity corresponding to ‘Service1’. Each organisation controls access to its own resources and services. It is responsible for the authentication of its own users, and for their use of services hosted by other organisations. Fourth, at the invocation step, Alice wants to use ‘Service1’; she is first authenticated by ‘A’. This request involves an access (controlled by A’s OrBAC policy) to the local object ‘ws-image1’ representing ‘Service1’, as well as a remote access (controlled by B’s OrBAC policy) to B’s actions corresponding to ‘Service1’. Both A’s and B’s CIS check that all exchanges between ‘A’ and ‘B’ are compatible with the agreed contract, and store a log of all exchanges to serve as evidence in case of dispute. If the invocation of ‘Service1’ is authorised, ‘A’ sends a SOAP/XML request to the URL of ‘Service1’, ‘B’ executes the request, and sends back the result of ‘Service1’ to ‘A’, and then ‘A’ transmits this result to ‘Alice’.

Figure 2 General architecture of PolyOrBAC



Source: Baïna et al. (2009)

Figure 3 Notion of virtual user and WS image (see online version for colours)



Source: Baïna et al. (2009)

In another research work (He, 2015), authors present virtual resource provision based on elastic reservation in cloud computing. In cloud platforms, resource provision service plays an important role to provide flexible and reliable IT-infrastructure for various kinds of applications. Unfortunately, current resource provision service seldom support resource reservation which is generally applied for improving the quality of service (QoS) in high-performance systems. To address this problem, a virtual machine provision policy based on elastic reservation mechanism is proposed. It extends the conventional 'on-demand provision' by introducing a novel elastic reservation mechanism, which allows cloud providers to accept user's over-reservation requests under certain conditions so as to improve the resource effective utilisation and user's satisfaction. Theoretical analysis presents the approach to calculating the probability of elastic reservation, and experimental evaluation validates the effectiveness of the proposed policy and the effects of key parameter on system performance. The results show that comparing with existing techniques, elastic reservation-based resource provision policy can significantly increase the resource effective utilisation, and decrease the 'short-term resource under-provision' caused by excessively reservations. Another interesting research work (Zarvic et al., 2010) presents a task-resource dependency perspective on partner selection during the formation of networked business constellations. The organisational forms of networked business constellations in general are often interpreted as the new organisational forms of the 21st century. As far as such forms consist of multiple collaborating businesses, partner selection during the formation phase of a networked business constellation is a crucial task for successful operation in the future. We propose to choose the appropriate business partners by applying concepts from coordination theory. In particular, we decompose an identified business opportunity, usually an innovative product or service, into its embracing tasks and resources. These represent the competencies needed for meeting the business opportunity. The methodological approach for partner selection is discussed from a task-resource dependency perspective and the benefits for the networked business context are highlighted. The research in this paper is accompanied by an argumentation-based validation, as well as by an evaluation of sustainability.

In a different way, the authors in Bhat et al. (2017) aims to explain that it is vital for any organisation to understand the abilities of their employees which help them to function in a competent manner. Exploratory research method has been used for the study and factors affecting trust, information sharing and communication, in virtual teams were extracted. This study segregates the virtual team members on the basis of the score given to them by their managers on the factors identified. These composite scores are subjected to K-means cluster analysis where every cluster profile extracted, represents a detailed summary of the employees in the cluster. This forms the basis for creation of this tool – the employee profile configurator. The tool helps organisations and managers to identify the unique characteristics of the employees to classify them accordingly in a specific cluster (Bhat et al., 2017). Another study (Mattos and Laurindo, 2015) aims to analyse the virtuality as a measurable construct along three dimensions (internal customers, external customers and suppliers), characterising companies according to their virtuality level. Cluster analyses were applied to achieve this aim. The results reveal three major groups differentiated by the type of information technology tools adopted, transactional versus collaborative profile and performance perceived by managers. This study indicated several managerial implications. First, only 31% of the companies analysed are applying tools in different dimensions (internal customer, suppliers and customers) to interact and conduct business in a synchronised and synergistic form aligned with the concept of a VO. Second, the group of companies that present a higher level of virtuality have a perceived improvement in performance by managers (Mattos and Laurindo, 2015).

4 Interoperability proposition

The next aspect that we want to address is interoperability between the possible heterogeneous entities that collaborates inside a CI. Indeed, in PolyOrBAC, all entities have to use WS (soap/WSDL) technology, one can easily imagine that this collaboration have to be more loose and agile. In this same scope, we intent to use UEML in order to propose a first proposition for interoperability issues management in CIs. The Sections 4.1 and 4.2 are based on Panetto et al. (2004).

4.1 UEML and the need for meta-modelling

The UEML project (http://www.ueml.org) was set up in an attempt to contribute to the solving of the problems of multiple EMLs. The long-term objective of UEML is the definition of a core language called UEML, which would serve as an Interlingua between EM tools. This language will:

- Provide the business community with a common visual, template-based language to be used on top of most commercial enterprise modelling and workflow software tools.
- Provide standardised mechanisms for sharing and exchanging enterprise models among projects, overcoming tool dependencies.
- Support the implementation of open and evolutionary enterprise model repositories to leverage enterprise knowledge engineering services and capabilities.

In order to prepare this long-term objective, the UEML project was initiated with the objective to create and manage a working group aiming to:

- Create a European Consensus on a core set of modelling constructs and facilitating interoperability in the frame of on-going standardisation efforts in this domain.
- Build a demonstrator portal with services and contents to support and promote, testing, industrial validation, and to collect comments. The first objective of the project was to analyse the market potential of a UEML, to accurately define the specifications of an embryo of such a language and to demonstrate and disseminate the concepts.

However, its syntax is not well defined and therefore it cannot be used as an exchange format between distinct tools. It also does not define mappings between existing EMLs and itself. The usefulness of a UEML would therefore reside in the availability of a well-defined syntax and well defined mappings (possibly standardised) between various EMLs and UEML. Panetto et al. (2004) believe that the definition of mappings between languages and UEML is important but quite independent from the UEML definition itself. Thought, they should be precisely defined and shared (through, for instance, standardisation); they should base on reasonable hypotheses and will never be fully (and formally) provable. Other approaches which attempt to solve the problems of exchange and interoperability between computerised systems do not deal clearly with the enterprise modelling area. They can be classified as ways for enabling business level communication between distinct computer-based systems and therefore as bottom-up approaches. However, another prerequisite for the exchange of models (or to make models interoperable) through a common language to be meaningful is to clearly understand the semantic links existing between the models themselves. This understanding is fundamental because without it, an exchanged model could be understood in a totally different way by the receiving tool, and thus misinterpreted.

In order to understand the links between distinct languages, meta-modelling is an important issue. Meta-modelling allows defining the syntax of a language. The product of meta-modelling is usually called a meta-model. Meta-models need to be described by using meta-modelling techniques (i.e., languages for making meta-models). These techniques are content-independent (applicable for the definition of any language). Currently, several meta-modelling languages (and also tools) exist but none of them are specifically targeted for the definition of EMLs. The reason is that these meta-modelling languages were often developed to design and implement information systems, knowledge base systems and computer-based infrastructures (environments) allowing to program meta-models.

4.2 The UEML approach and defining mappings among EMLs

In the UEML project, a meta-model may also be used to define part or all of the semantics of the language. But this is often not recommended. It should be noted that the notion of meta-modelling technique is relative. In fact, it is often true that a language can be used as a meta-modelling technique for another (sometimes, the same) language (namely IEM, EEML and GRAI). First, models of this scenario where elaborated in the three distinct languages and the exchange was performed manually by specialists of these languages. More precisely, given a first model in IEM, specialists of GRAI and EEML provided the ‘semantically equivalent’ model in their own languages. Afterward, IEM, EEML and GRAI constructs have been meta-modelled using UML class diagram. This resulted in three so-called ‘original meta-models’. At the same time, the links between the concepts of every original meta-model and their use in the models of the scenario were defined to illustrate how a unique real-world phenomenon is modelled with the three original meta-models. With the aim to define a common meta-model for core constructs, (Panetto et al., 2004) compared and ‘unified’ the three meta-models through an incremental approach. They compared the three meta-models peer-to-peer to find any correspondence between a concept in one meta-model and a concept in another one. Once the peer-to-peer correspondences (and absence of correspondences) had been defined, a set of common concepts were identified (Table 1) and further elaborated into the first version of the UEML meta-model 1.0 (Figure 4).

This meta-model represents the common concepts underlying the three original EMLs. This meta-model being remarkably different from the three meta-models by the use of an appropriate higher level of abstraction and considering some discrepancies among the three original meta-models, (Panetto et al., 2004) informally re-defined new correspondences between the UEML meta-model and each original meta-model. The clear definition of the meta-models of existing EMLs and of UEML with meta-modelling techniques is necessary but not sufficient to achieve a meaningful exchange of models. The correspondences among constructs between two distinct languages have to be precisely defined by comparing semantics of these constructs. However, this is a difficult task because:

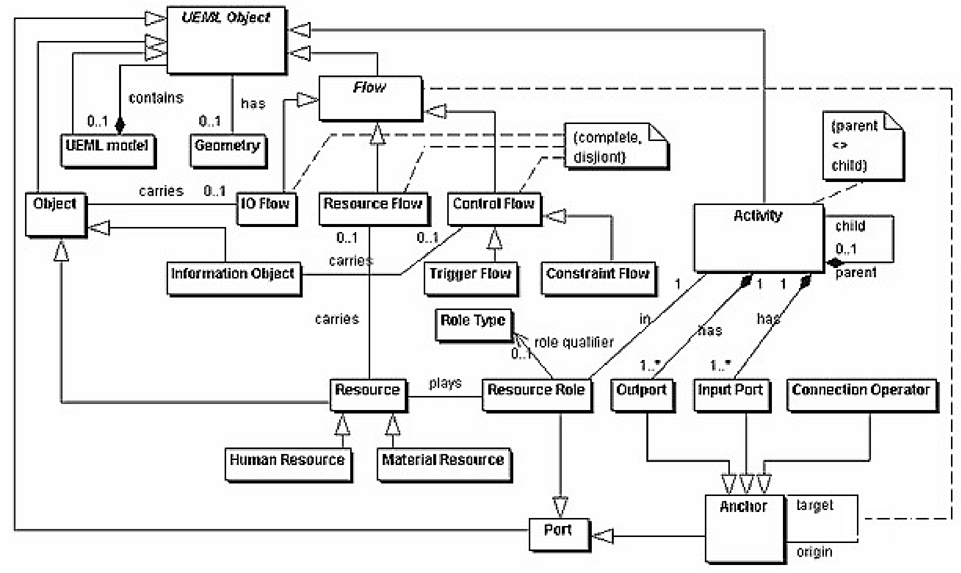
- EMLs are often based on informal semantics, i.e., some natural descriptions of constructs meaning.
- The way in which EMLs are used in specific context and situations may change.

Table 1 Extract of the common concepts of UEML

Common concept	*GRAI*	*IEM*	*EEML*
Activity	Extend activity	Action state	Task
Role	Not explicit	IEM object state	Role
Resource	Resource	Resource class	Resource
Input/output flow	Input/flow Output/flow	Successor/process element	Flow (control flow = false)
Constraint flow	Control flow (trigger = false)	No direct	Flow (control flow = false and linked to role)
Control flow	Control flow (trigger = true)	Control successor/ process element	Flow (control flow = true)
Resource flow	Resource flow (trigger = false)	Resource successor/ resource state	Role (linked to task)
Connection operator	Logical operator	Connection element state	Decision point (not import or outport)
Port	Connector	Port	Decision point (import or outport)

Source: Panetto et al. (2004)

Figure 4 The UEML 1.0 meta-model



Source: Panetto et al. (2004)

Therefore, as suggested previously, mappings between languages should rely on reasonable hypotheses should be clearly stated and become the base for building the language, and possibly be standardised further. Mappings can be defined, more or less precisely, in various languages. For example, they can be expressed informally in natural language or through the use of a meta-modelling language. Defining relationships at the language level can also be done in an ‘a priori’ manner when new methodologies and methods are under definition.

Therefore, a UEML can be a good starting base for placing under control the process of defining new methods and methodologies as well as the rules applied in a specific methodology.

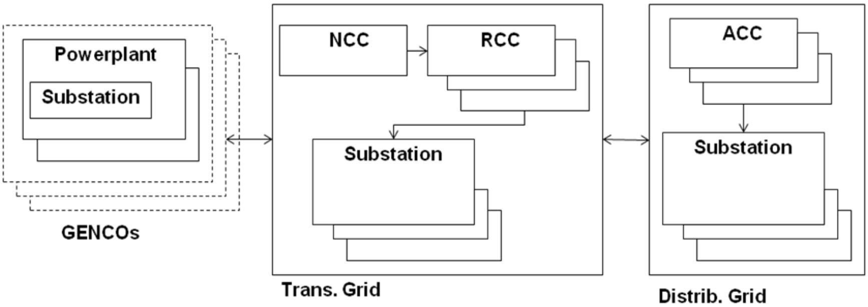
5 Application of PolyOrBAC to the electric power grid CII

We address here a case study showing how PolyOrBAC can be applied to an electrical power grid CII and how the UEML model could be instantiated with our electrical grid scenario. Sections 5.1 and 5.2 are based on Baina et al. (2009).

5.1 Electrical power grid architecture and scenarios

First of all, we give a description of the electrical power grid architecture.

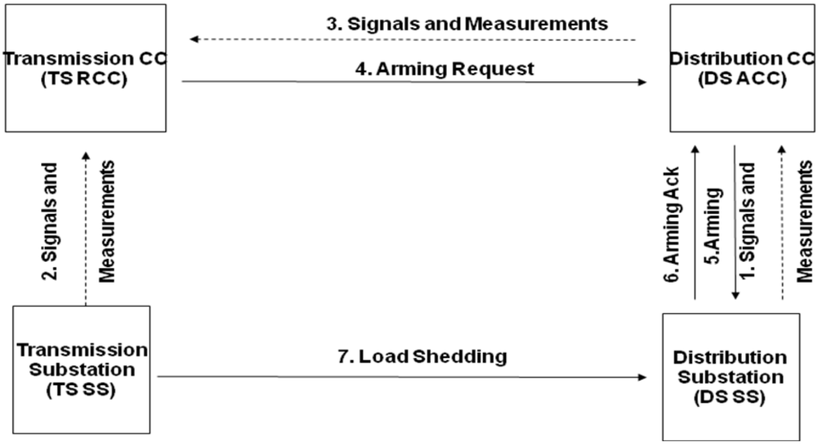
Figure 5 General architecture of an electrical power grid



Source: Baïna et al. (2009)

One or more electricity generation company (GENCO) – each in charge of several power plants – is connected to one or more transmission grids. Each transmission grid [managed by transmission system operators (TSO)] is composed of transmission substations (monitored by one national and several regional control centres), and is connected to one or more distribution grid. Finally, each distribution grid (managed by DSO) is composed of distribution substations (monitored by area control centres), and distributes electricity to subscribers (industries and habitations) over distribution lines (Garrone et al., 2007). PolyOrBAC is useful when some components of the electrical and information infrastructure execute remote actions and access to resources from other partner organisations. To correctly illustrate the application of PolyOrBAC on the electrical power grid CII, we study a practical scenario. This scenario considers the possible cascading effects due to ICT threats to the communication channel among TSO/DSO control centres and their substations in emergency conditions (e.g., line overloads). It is assumed that in emergency conditions the TSO is authorised by the DSO to activate defence plan actions for performing load shedding activities on the distribution grid. By studying this scenario, we distinguish four important classes of organisations: transmission regional control centres (TS RCC) that are managed by TSOs, transmission substations (TS SS), distribution area control centres (DS ACC) that are managed by DSOs, and distribution substations (DS SS). Figure 6 details the most important commands and signals exchanged between these Organisations in normal and emergency situations.

Figure 6 Exchanged commands and signals


Transmission CC (TS RCC)
3. Signals and Measurements
4. Arming Request
Distribution CC (DS ACC)
2. Signals and Measurements
6. Arming Ack
5.Arming
1. Signals and Measurements
Transmission Substation (TS SS)
7. Load Shedding
Distribution Substation (DS SS)

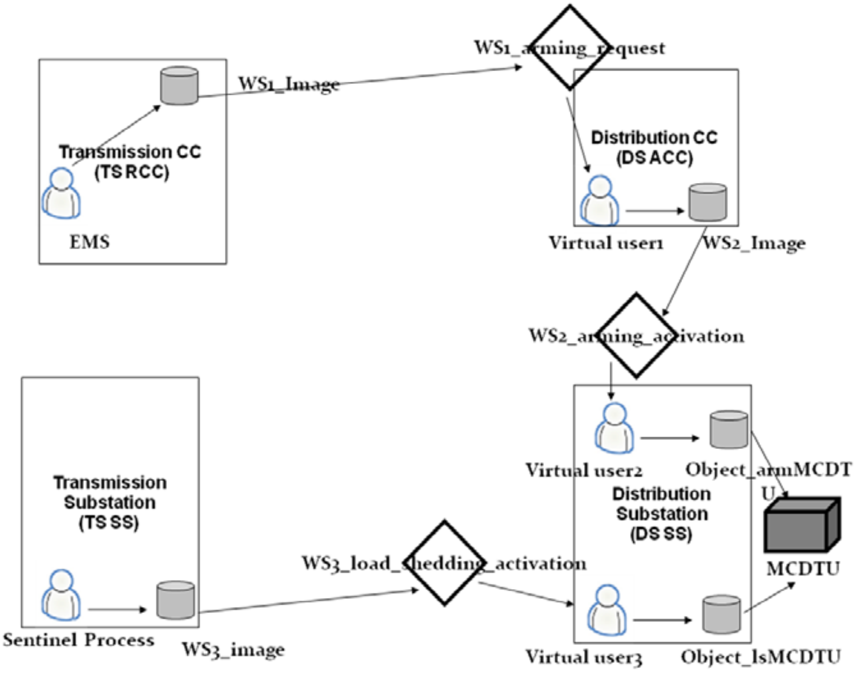
Source: Baïna et al. (2009)

In normal operation, all DS SSs send several signals and measurements (power, voltage, frequency) to the TS RCC via their DS ACC (1) and (3). On the other hand, all TS SSs send various signals and measurements (power, voltage, frequency) to their TS RCC (2). The TS RCC monitors the electric power system and elaborates some potentially emergency conditions that could be remedied with opportune load shedding commands applied to particular areas of the grid. In order to actuate the defence action, the TS RCC chooses, for arming, a subset of high voltage (HV)/medium voltage (MV) DS SSs from the list of participating DS SSs to the emergency plan. In the arming step, the TS RCC sends the requests of preventively arming these DS SSs to the interested DS ACCs. (4), in order to prepare the possible upcoming load shedding. These DS ACCs send the arming order to DS SSs which will arm then the right electrical component (called MCDTU) (5), and the armed DS SSs send an acknowledgement to DS ACC (6). MCDTU stands for ‘monitoring control and defence terminal unit’. In case of detection of a real emergency situation, the TS SS sends a load shedding command to all DS SSs participating to the emergency plan, and only the previously armed DS SSs will perform load shedding over their MCDTUs (7).

5.2 Electrical scenario interpretation with PolyOrBAC

Let us detail the invocations of the involved WS in the scenario described above, according to PolyOrBAC security policy (Figure 7).

Figure 7 PolyOrBAC approach applied to the electrical scenario (see online version for colours)



Source: Baïna et al. (2009)

5.3 Instantiating the UEML model with our electric grid scenario

This section is based on Baina et al. (2009) and Panetto et al. (2004). In normal operation, all DS SSs send several signals and measurements (power, voltage, frequency) to the TS RCC via their DS ACC (1) and (3). On the other hand, all TS SSs send various signals and measurements (power, voltage, frequency) to their TS RCC (2).

Table 2 Common and instantiated concepts for arming distribution stations' at TS CC

Common concept	Instantiated concept
Activity	Arming distribution stations
Resource	Transmission centre
Input/output flow	Soap message
Constraint flow	Signals and measurements from DS CC
Control flow	Arming distribution stations through DS CC
Resource flow	DS CC, TS SS
Connection operator	CIS
Port	http

The TS RCC monitors the electric power system and elaborates some potentially emergency conditions that could be remedied with opportune load shedding commands applied to particular areas of the grid. In order to actuate the defence action, the TS RCC chooses, for arming, a subset of HV/MV DS SSs from the list of participating DS SSs to the emergency plan. In the arming step, the TS RCC sends the requests of preventively arming these DS SSs to the interested DS ACCs. (4), in order to prepare the possible upcoming load shedding.

Table 3 Common and instantiated concepts for arming distribution stations' at DS CC

Common concept	Instantiated concept
Activity	Arming distribution stations
Resource	Distribution centre
Input/output flow	Soap message
Constraint flow	Signals and measurements from DS SS
Control flow	Arming distribution stations
Resource flow	Distribution stations
Connection operator	CIS
Port	http

Table 4 Common and instantiated concepts for 'signals and measurements, load shedding distribution stations' at TS SS

Common concept	Instantiated concept
Activity	Signals and measurements, load shedding distribution stations
Resource	Transmission substations
Input/output flow	Soap message
Constraint flow	Emergency conditions
Control flow	Load shedding
Resource flow	Distribution stations
Connection operator	CIS
Port	http

Table 5 Common and instantiated concepts for 'signals and measurements, arming ack' at DS SS

Common concept	Instantiated concept
Activity	Signals and measurements, arming acknowledgment (ack)
Resource	Distribution substations
Input/output flow	Soap message
Constraint flow	Being armed
Control flow	Locally execute the load shedding
Resource flow	THIS (local object)
Connection operator	CIS
Port	http

These DS ACCs send the arming order to DS SSs which will arm then the right electrical component (called MCDTU) (5), and the armed DS SSs send an acknowledgement to DS ACC (6).

In case of detection of a real emergency situation, the TS SS sends a load shedding command to all DS SSs participating to the emergency plan, and only the previously armed DS SSs will perform load shedding over their MCDTUs (7).

In this section, we have presented the UEML model for interoperability, and we have instantiated this latter with our electric grid scenario extracted for a real CI scenario proposed by the European project CRUTIAL (Dondossola et al., 2006). UEML will serve as an intermediary between enterprise modelling tools providing the business community with a common visual, template-based language to be used on top of most commercial enterprise modelling and workflow software tools, and more particularly in the context of CII that have interoperability and collaboration needs.

6 Conclusions and extensions

This paper presents a security framework which meets the requirements of access control and collaboration of CIIs. PolyOrBAC manages collaboration and resources sharing between all organisations of a CII thanks to the WS technology, while controlling that the interactions between these organisations are in conformity with their needs and their internal security policies specified thanks to OrBAC. Through the use of WS technology, PolyOrBAC offers a decentralised management of the access control policies and an architecture where organisations mutually negotiate the contracts for collaboration. The coupling between organisations is weak (loose coupling), and each organisation keeps its own resources, services, applications, operating system, functioning rules, goals and security policy rules (specified according to OrBAC). Each organisation is responsible for the authentication of its users and is liable for their use of other organisations' services; it also controls the access to its own resources and services. The WS technology allows communications between organisations without intimate knowledge of each other's IT systems location or composition; moreover, even if remote accesses are possible, it is not necessary to know the hierarchical structure of the other organisations. PolyOrBAC can thus ensure privacy and non-disclosure of data and services. The extensibility and the usability of WS and OrBAC, facilitate the management and the integration of new organisations (with their users, data, services, policy). Moreover, PolyOrBAC handles heterogeneity of hardware and software, and there is no constraint for type, or location of hardware/software. Network segments or physical/logical equipments can be assimilated to organisations (network, firewall, gateways, routers, IDS, OS, DBMS, etc.) (Cuppens et al., 2005). To check the feasibility of our approach, an implementation is currently carried out on a JAVA environment using the Eclipse IDE. More details about this implementation will be presented soon. The other aspect that we wanted to address is interoperability between the possible heterogeneous entities that collaborates inside a CI. Indeed, in PolyOrBAC, all entities have to use WS (soap/W technology, one can easily imagine that this collaboration have to be more loose and agile. In this same scope, we used UEML in order to propose a first proposition for interoperability issues management in CIs. Our approach is limited by the fact that it does not yet take into account availability of data and services, and criticality levels for all the components that are integrated in the CI. This approach can be extended by taking into account availability and integrity requirements. For integrity, our approach can be extended to monitor information flows, and prevent flows from low-criticality tasks to high criticality tasks, except when such flows are validated by means of adequate fault-tolerance mechanisms (Totel et al., 1998). In this regard, we have developed three models: trust, criticality and availability management. The security of telecommunications infrastructures is a major issue for satisfied it in terms of confidentiality, integrity and availability also in terms of QoS; they present the vulnerabilities such as security breach, default conception or configuration. These systems break down, suffer in use from errors and attack from outside or inside by pirates and cyber criminals. The global approach of security in systems is essential for the privacy protection, to defend the patrimony from the company or reduce vulnerabilities of large information systems. Our proposition for criticality management (Kasmi et al., 2016) presents different aspects of security, threats and vulnerabilities in IP multimedia subsystem (IMS) networks and issues for QoS management. Hence, not only QoS but also resilience of the services and networks are needed. In this regard, we propose incorporation a layer above the QoS controller based on fuzzy logic to determine the guaranteed levels of QoS according to levels of criticality. It describes a new approach of multi criticality in order to ensure the integrity in IMS networks and reduce the interdependencies impacts by applying resilience strategy. This approach is based on the recent model of integrity total. Availability can be handled by means of obligation rules, to provide enough resources to achieve requested activities, even in case of events such as component failures or attacks. Our model for managing availability (Bakraouy et al., 2017) presents our contribution that is devoted to the integration of SMA in cloud computing. The role and functionality of each which constitute our system is detailed. We realised an SMA-based cloud computing system for the classification and the automatic negotiation of SLAs. Trust negotiation is an approach to establishing trust across security domains in a dynamic coalition in real-time through the bilateral exchange of digital credentials. This is accomplished through the use of access control policies that specify what combinations of digital credentials a stranger must disclose to gain access to a coalition resource. Some existing works on trust negotiation (Seamons et al., 2003) and trust-based access control (Adams and Davis, 2005) will help us in the future to develop our negotiation step. Ensuring the security of the information systems in the collaborative systems presents a priority for governments, given their crucial role in the success of CIs. This security requires the establishment of the trust between the participating entities and it requires also the access control to the resources in other organisations. In this regard, we have developed a new trust negotiation model named Tr-OrBAC (Aali et al., 2015), this model is based on the application of AHP method to evaluate the trust according to a specific collaboration context and then to generate the trust rules. Our goal is to enable to each organisation to evaluate the trust of different entities in other organisations. According to this evaluation, the collaboration decision will be decided. This decision is translated to a set of generated trust rules by applying the principle of OrBAC model for access control. In this model we add a new variable expressing the result of the trust evaluation. Our general framework will able organisations (more particularly in a CII) that insists on having a fine grained access control (OrBAC), collaboration (WS), interoperability (UEML), availability, and criticality requirements to fulfil their objectives in a holistic and coherent approach.

References

Aali, N.A., Baïna, A. and Echabbi, L. (2015) 'Tr-OrBAC: a trust model for collaborative systems within critical infrastructures', in the *5th World Congress on Information and Communication Technologies (WICT 2015)*, Marrakesh, Morocco, pp.123–128, DOI: 10.1109/WICT.2015.7489657.

Adams, W.J. and Davis, N.J. (2005) 'Toward a decentralized trust-based access control system for dynamic collaboration', in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, pp.317–324, https://doi.org/10.1109/IAW.2005.1495969.

Alawamleh, M. and Popplewell, K. (2012a) 'Analysing virtual organisation risk sources: an analytical network process approach', *International Journal of Networking and Virtual Organization*, Vol. 10, No. 1, pp.18–39.

Alawamleh, M. and Popplewell, K. (2012b) 'Risk in virtual organisation: a case study', *International Journal of Networking and Virtual Organization*, Vol. 11, No. 2, pp.142–155.

Amin, M. (2003) 'North America's electricity infrastructure: are we ready for more perfect storms?' *IEEE Security and Privacy*, pp.19–25, https://doi.org/10.1109/MSECP.2003.1236231.

Baïna, A., El Kalam, A.A., Deswarte, Y. and Kaaniche, M. (2009) 'Collaborative access control for critical infrastructures', in *Critical Infrastructure Protection II*, pp.189–201, Springer, Arlington, VA, USA.

Bakraouy, Z., Baïna, A. and Bellafkih, M. (2017) 'System multi agents for automatic negotiation of SLA in cloud computing', Paper presented at the *13th International Conference on Information Assurance and Security (IAS)*, Marrakech, Morocco, under Publication.

Bell, D.E. and LaPadula, L.J. (1976) *Secure Computer Systems: Unified Exposition and MULTICS Interpretation*, ESD-TR-75-306, MTR 2997 Rev.1, MITRE Corp., USA.

Bhat, S.K., Pande, N. and Ahuja, V. (2017) 'Employee profile configurator: a tool to improve effectiveness of a virtual team', *International Journal of Networking and Virtual Organization*, Vol. 14, No. 4, pp.392–409.

Brose, G. (1999) 'A view-based access control model for CORBA', in *Secure Internet Programming, Lecture Notes in Computer Science*, pp.237–252, Springer, Berlin, Heidelberg, https://doi.org/10.1007/3-540-48749-2_10.

Correia Alves, O. and Rabelo, R.J. (2013) 'A KPI model for logistics partners' search and suggestion to create virtual organisations', *International Journal of Networking and Virtual Organization*, Vol. 12, No. 2, pp.149–177.

Cuppens, F., Cuppens-Boulahia, N., Sans, T. and Miège, A. (2005) 'A formal approach to specify and deploy a network security policy', in *Formal Aspects in Security and Trust, IFIP International Federation for Information Processing*, pp.203–218, Springer, Boston, MA, https://doi.org/10.1007/0-387-24098-5_15.

Daassi, M., Jawadi, N., Favier, M. and Kalika, M. (2006) 'An empirical investigation of trust's impact on collective awareness development in virtual teams', *International Journal of Networking and Virtual Organization*, Vol. 3, No. 4, pp.378–394, https://doi.org/10.1504/IJNVO.2006.011867.

Dondossola, G., Deconinck, G., Di Giandomenico, F., Donatelli, S., Kaâniche, M. and Verissimo, P. (2006) 'Critical utility infrastructural resilience', in *International Workshop on Complex Network and Infrastructure Protection (CNIP-06)*, Rome, Italy, 12p.

Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R. and Chandramouli, R. (2001) 'Proposed NIST standard for role-based access control', *ACM Transactions on Information and System Security*, Vol. 4, No. 3, pp.224–274, https://doi.org/10.1145/501978.501980.

Fink, T., Koch, M. and Oancea, C. (2003) 'Specification and enforcement of access control in heterogeneous distributed applications', in *Web Services – ICWS-Europe 2003, Lecture Notes in Computer Science*, pp.88–100, Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-540-39872-1_8.

Garrone, F., Brasca, C., Cerotti, D., Codetta Raiteri, D., Daidone, A., Deconinck, G., Donatelli, S., Dondossola, G., Grandoni, F., Kaâniche, M. and Rigole, T. (2007) *Analysis of New Control Applications*, CRUTIAL project, Deliverable D2.

He, H. (2015) 'Virtual resource provision based on elastic reservation in cloud computing', *International Journal of Networking and Virtual Organization*, Vol. 15, No. 1, pp.30–47.

Ignatiadis, I., Svirskas, A., Roberts, B. and Tarabanis, K. (2006) 'Promoting trust in B2B virtual organisations through business and technological infrastructures', *International Journal of Networking and Virtual Organization*, Vol. 3, No. 4, pp.395–411, https://doi.org/10.1504/IJNVO.2006.011868.

Kalam, A.A.E., Baida, R.E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miège, A., Saurel, C. and Trouessin, G. (2003) 'Organization based access control', in *IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, pp.120–131, https://doi.org/10.1109/POLICY.2003.1206966.

Kalam, A.A.E., Deswarte, Y., Baïna, A. and Kaaniche, M. (2007) 'Access control for collaborative systems: a web services based approach', in *IEEE International Conference on Web Services (ICWS 2007)*, pp.1064–1071, https://doi.org/10.1109/ICWS.2007.30.

Karakostas, B. (2014) 'Cloud architecture for dynamic virtual organisations in transport logistics', *International Journal of Networking and Virtual Organization*, Vol. 13, No. 2, pp.146–158.

Kasmi, O., Baïna, A. and Bellafkih, M. (2016) 'Multi-level integrity management in critical infrastructure', in *11th International Conference on Intelligent Systems: Theories and Applications (SITA 2016)*, Mohammedia, Morocco, pp.1–6, DOI: 10.1109/SITA.2016.7772292.

Khan, M.S. (2012) 'Role of trust and relationships in geographically distributed teams: exploratory study on development sector', *International Journal of Networking and Virtual Organization*, Vol. 10, No. 1, pp.40–58, https://doi.org/10.1504/IJNVO.2012.045210.

King, J. and Kawash, J. (2011) 'A real-time XML protocol for bridging virtual communities', *International Journal of Networking and Virtual Organization*, Vol. 9, No. 3, pp.248–264, https://doi.org/10.1504/IJNVO.2011.042482.

Laprie, J.C., Kanoun, K. and Kaâniche, M. (2007) 'Modelling Interdependencies between the electricity and information infrastructures', *International Conference on Computer Safety, Reliability, and Security*, Trento, Italy, pp.57–67.

Lorch, M., Proctor, S., Lepro, R., Kafura, D. and Shah, S. (2003) 'First experiences using XACML for access control in distributed systems', in *Proceedings of the ACM Workshop on XML Security*, New York, NY, USA, pp.25–37, https://doi.org/10.1145/968559.968563.

Mattos, C.A.D. and Laurindo, F.J.B. (2015) 'Measuring virtuality in an organisational context: a quantitative study of Brazilian manufacturing companies', *International Journal of Networking and Virtual Organization*, Vol. 15, Nos. 2–3, pp.256–276.

Namin, A.S., Shen, W. and Ghenniwa, H. (2006) 'Implementing enterprise collaboration using web services and software agents', *International Journal of Networking and Virtual Organization*, Vol. 3, No. 2, pp.185–201, https://doi.org/10.1504/IJNVO.2006.009534.

Noran, O. (2006) 'Refining a meta-methodology for collaborative networked organisations: a case study', *International Journal of Networking and Virtual Organization*, Vol. 3, No. 4, pp.359–377, https://doi.org/10.1504/IJNVO.2006.011866.

OASIS (2005) *UDDI, UDDI Specifications* TC, February 2005.

Panetto, H. (2004) 'A unified enterprise modelling language for enhanced interoperability of enterprise models', *IFAC Proc.*, Vol. 37, pp.605–610, https://doi.org/10.1016/S1474-6670(17)36181-5.

Panetto, H., Berio, G., Benali, K., Boudjlida, N. and Petit, M. (2004) 'A unified enterprise modelling language for enhanced interoperability of enterprise models', *11th IFAC Symposium on Information Control Problems in Manufacturing (INCOM 2004)*, Salvador, Brazil, Vol. 37, pp.605–610 [online] https://doi.org/10.1016/S1474-6670(17)36181-5.

Petersen, S.A. (2007) 'Virtual enterprise formation and partner selection: an analysis using case studies', *International Journal of Networking and Virtual Organization*, Vol. 4, No. 2, pp.201–215.

Preis, M. and Seitz, J. (2012) 'Challenges and conflicts integrating heterogeneous data warehouses in virtual organisations', *International Journal of Networking and Virtual Organization*, Vol. 11, Nos. 3–4, pp.329–344, https://doi.org/10.1504/IJNVO.2012.048914.

Rinaldi, S.M., Peerrenboom, J.P. and Kelly, T.K. (2001) 'Identifying, understanding, and analysing: critical infrastructure interdependencies', *IEEE Control Systems, Control of Complex Networks*, Vol. 21, No. 6, pp.11–64.

Sainan, L. (2010) 'Task-role-based access control model and its implementation', in *2nd International Conference on Education Technology and Computer*, pp.293–296, https://doi.org/10.1109/ICETC.2010.5529541.

Sandhu, R.S., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (1996) 'Role-based access control models', *Computer*, Vol. 29, pp.38–47, https://doi.org/10.1109/2.485845.

Seamons, K.E., Chan, T., Child, E., Halcrow, M., Hess, A., Holt, J., Jacobson, J., Jarvis, R., Patty, A., Smith, B., Sundelin, T. and Yu, L. (2003) 'TrustBuilder: negotiating trust in dynamic coalitions', in *Proceedings DARPA Information Survivability Conference and Exposition*, Vol. 2, pp.49–51, https://doi.org/10.1109/DISCEX.2003.1194912.

Shamsuzzoha, A. and Helo, P.T. (2015) 'Virtual business process management within collaborative manufacturing network: an implementation case', *International Journal of Networking and Virtual Organization*, Vol. 14, No. 4, pp.319–339.

Totel, E., Blanquart, J.P., Deswarte, Y. and Powell, D. (1998) 'Supporting multiple levels of criticality, in: digest of papers', *Twenty-Eighth Annual International Symposium on Fault-Tolerant Computing* (Cat. No. 98CB36224) pp.70–79 https://doi.org/10.1109/FTCS.1998.689456.

Verginadis, Y., Apostolou, D., Papageorgiou, N. and Mentzas, G. (2011) 'OCEAN: an ontology for supporting interoperability service utilities in virtual organisations', *International Journal of Networking and Virtual Organization*, Vol. 9, No. 2, pp.184–209.

W3C, SOAP (2003) *W3C Recommendation*, June 2003.

W3C, WSDL (2006) *W3C Candidate Recommendation*, March 2006.

W3C, XML (2004) *W3C Recommendation*, February 2004.

Walker, H. (2006) 'The virtual organisation: a new organisational form?', *International Journal of Networking and Virtual Organization*, Vol. 3, No. 1, pp.25–41.

Wognum, P.M. and Faber, E.C.C. (2002) 'Infrastructures for collaboration in virtual organisations', *International Journal of Networking and Virtual Organization*, Vol. 1, No. 1, pp.32–54.

Wu, Y. 'Andy', and Li, Y. (2009) 'Inter-organisational trust in B2B commerce', *International Journal of Networking and Virtual Organization*, Vol. 6, No. 3, pp.303–317.

Yen, D., Chou, D.C., Chen, T. and Chen, H-G. (2002) 'Becoming a virtual organisation: a strategic approach', *International Journal of Networking and Virtual Organization*, Vol. 1, No. 2, https://doi.org/10.1504/IJNVO.2002.002545.

Zarvic, N., Seifert, M. and Thoben, K-D. (2010) 'A task-resource dependency perspective on partner selection during the formation of networked business constellations', *International Journal of Networking and Virtual Organization*, Vol. 7, No. 5, pp.319–414.

Notes

[1] A failure in one infrastructure causes the failure of one or more components in a second infrastructure.

[2] When an existing failure in one infrastructure exacerbates an independent failure of a second infrastructure, generally in the form of increasing the severity or the time for recovery or restoration of the second failure.