# Maintenance & Information Security Ontology

SI AHMED Boualem
Dept: Génie Industrielle
Ecole Nationale Polytechnique d'Alger
boualem.si-ahmed@g.enp.edu.dz

BERRANI Meryem
Dept: Génie Industrielle et Maintenance
Ecole Nationale Superieure de Technologie
Alger, Algérie
Meryem.berrani@gmail.com

Nibouche Fatima
Dept: Génie Industrielle
Ecole Nationale Polytechnique d'Alger
fatima.nibouche@g.enp.edu.dz

***Abstract*— the aim of the Ontology named MISO (Maintenance & Information Security Ontology) is to conceptualize the interaction between industrial maintenance and safety information while respecting the requirements of the ISO 2700x standard.**

**The interest of this approach is to help maintenance and/or information security operators to understand the relation between them, especially during execution of an operation of maintenance. For the first one the interest is to know how not to influence information and its security and for the second one, what to control to minimize the risks indicated by the current operation.**

**Our work is based on the method UPON Lite, the tools used are StarUML for conceptualizing, Secure 4.3 for ontologization and operationalization, the JENA inference engine in collaboration with NetBeans. And for the ontology interrogation SPARQL queries with a user interface has been developed.**

***Keywords*— *Maintenance, Information Security, Ontology, OWL, PROTÉGÉ 4.3, SPARQL, ISO2700x, UPON Lite, NetBeans,***

## I. Introduction :

. Industrial companies often operate in a competitive environment where everything is about productivity. In this situation, many organisations forget to think about securing information.

An alarming situation challenges us. Often companies do not take into account the risks related to information security (IS) during the realization of the maintenance operation, sometimes by lack of visibility or understanding.

In this game of cat and mouse, there are also organisations that use these maintenance operations to break into the information system and touch either the integrity, confidentiality, availability, or other security settings of the information systems.

A maintenance operation is defined in the AFNOR (2001) standard as following: 'Maintenance includes all technical, administrative, or managements that are intended to maintain or restore equipment in a state or data condition dependability to perform a required function',

Information security is defined in ISO CEI 27001 as 'Preservation of confidentiality, integrity and availability of information'

We propose a conceptual model of the interactions between maintenance and information security system by developing ontology.

Bekkaoui et al. [1] developed ontology to choose an expert with a feedback experience to accomplish a maintenance task; the work was based on [2] CMDO ontology. Our model completes this vision by integrating information security.

Our contribution is to help the maintenance operator or information security operator, to understand the interaction between an activity of maintenance and the related information security's risks, vulnerabilities, and measures that they can applied to minimize their effect on the system. In fact they can ask for example: what are the risks on information security if I change the sensor of this machine? The ontology will, therefore permit to respond to such questions.

Through reasoning of property, ontologies logic, we can also in this universe derive other logical relationships to power in a second time interface to interact with the model.

The paper is structured as follow. In section II, we expose the state of the art of both maintenance ontologies and information security conceptualisation. In section III, we define the position of the problem of interaction between Maintenance activity and information security system. Section IV describe our Maintenance and Information Security Ontology (MISO). Finally, section V concludes and discusses future challenges.

## II. Overview maintenance and Information security ontologies

In this paper, we focus on two domains, Maintenance and Information security. The information has intrinsic value, especially in its exchange and sharing it develops value.

978-1-5090-6465-6/17/$31.00 ©2017 IEEE

Some of these concepts and definitions will be used in the construction of our ontology;

2.1 *Ontology:*

The term ontology has been used since the early 1990s in the fields of artificial intelligence (AI), in particular knowledge engineering and knowledge representation.

The literature contains several definitions for this term; as knowledge, which is tacit or explicit [3] and [4] define the ontology as an explicit specification of a conceptualization.

*2.2 Maintenance:*

*Activity / Action of maintenance:* whether preventive or corrective, the final goal is to keep the machine or more generally the system in working condition. It consists of a set of maintenance operations.

According to the [5], corrective maintenance is the "maintenance performed after failure", and the preventive maintenance is defined as "the maintenance performed according to predetermined criteria, in the intention of reducing the probability of failure". The figure below summarizes some concept of maintenance and the various relationships between them:

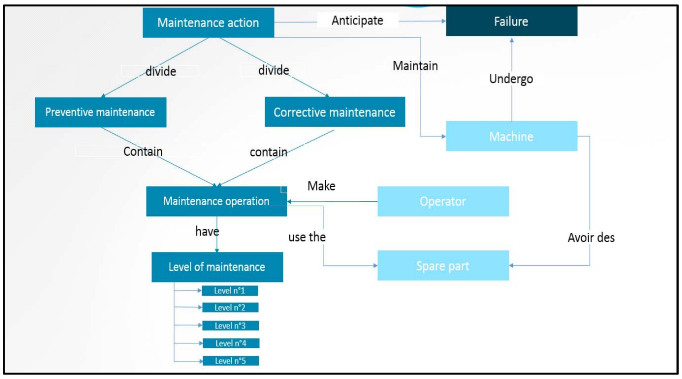


Fig.1. Interaction between maintenance concepts (this study)

In their different works Laallam, [6], Klai [7] and Anguel [8], had as goal, the establishment of a diagnostic support system.

[2] The management of maintenance as a function is also another aspect which was developed by Karray and his team, when in their publication, Philipp Saalmann and al [9] develop a set of ontologies, metadata, domain validation and then as a proper instance of a company taking an intelligent maintenance system integrating a spare parts supply chain planning. We developed ontology in management and especially in interaction with information security.

*2.3 Information security:*

Information security is based on three criteria, **integrity** is exact information without any non-authorized modification, **availability** is the access to the information exactly at the moment of need and **confidentiality** is the availability of the information exclusively for the authorized person or processes. In the state of the art we can find other criteria defined in the standard ISO

*2.4. Vulnerability:*

We find in the literature many definitions of the concept. Turki defined vulnerabilities as security holes in one or more systems. Any system seen as a whole has vulnerabilities that can be exploited or not [10].

It is defined by linking the concept of fault which exploitation may damage the s ystem [11].

*2.5. Threat*:

Any potential danger to information or systems [12].

*2.6. Risk*

Risk is unavoidable and present in every human situation. It is present in daily lives, public and private sector organizations. Depending on the context (insurance, stakeholder, technical causes), there are many accepted definitions of risk in use [13]. Barthélémy and al defined it as a situation (set of simultaneous or consecutive events) whose occurrence is uncertain and whose realization affects the company's goals [14].

*2.7. Information Security Management System (ISMS):*

The ISMS is a part of the overall management system, based on a risk approach related to the activity, to establish, implement, operate, monitor, review, maintain and improve information security.

It includes the organization, policies, planning activities, responsibilities, practices, procedures, processes and resources. The figure below summarizes some concept of information security and the various relationships between them:

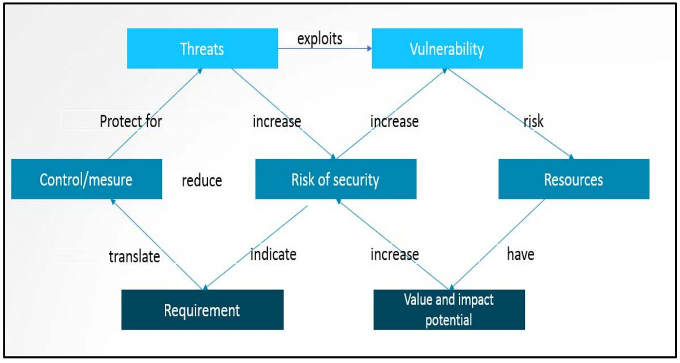


Fig. 2. Interaction between information security concepts [16]

Furthermore, concerning the security of information, there are a significant number of research works; we have, [15], [16] and [18], which follows the requirements of ISO 27001.

The works of Tung Ju Chiang and al [15], Fenz & al [16] and Thomas Neubauer & al [17], are interested to modeling for the first and second one, to audit Information Security Management System according to the ISO 27001 standard and for the last one the decision support system in the implementation of measurement ISO 27001 and other references and best practices.

Souag [18] classified information security ontologies into families for a better understanding of state of the art.

# III. problem of interaction between maintenance activity and information security management system:

Although it is difficult to attribute to these elements a book value loss, manipulation or theft of information, especially during a maintenance operation can significantly weaken a company and question its future prospects.

It is trivial that there is a relationship between the maintenance and security of information systems even more visible when the organization uses an external entity.

The race in innovation between countries to get the advanced technology has revealed several scandals related to industrial information were revealed this last years.

Simpler, an employee can lose information during a maintenance operation, erase data or destroy an equipment and lose information. We give below some interactions to explain these relations:

*Example 1 :*

The replacement of a sensor by an employee who has a weakness (vulnerability), in this case, lack of operator skill in this operation ”replacing the sensor”. There is a risk of bad positioning. This will affect the information that will be wrong or not available in either case, there could affect the production system or more generally on the company possibly causing financial loss.

Table 1. Example n°1 representing the interaction between the maintenance and IS

| **Maintenance operation** | Replacing the sensor. |
|---|---|
| **Interaction on information Security** | |
| **Information** | Information provided by the sensor such as temperature, pressure ... |
| **Risk** | Not available (or Integrity) of information |
| **Threat** | Wrong location of the sensor |
| **Vulnerability** | Operator skill Lack |

*Example 2 :*

During the maintenance operation "Screen change" there is a threat with a risk of disclosure of secret information such as the recipe; the cause is the vulnerability let the external operator unattended.

Table II. Interaction between change screen operation and information security

| **Maintenance operation** | Screen change |
|---|---|
| **Interaction on information Security** | |
| **Information** | the recipe |
| **Risk** | Disclosure of Information (Confidentiality) |
| **Threat** | Steal recipe |
| **Vulnerability** | External operator unattended |

***Example 3:***

During maintenance operation, the operator of maintenance cut an electric wire, there is a threat with a risk non-availability of information; the cause is vulnerability of external operator unattended.

Table III. Interaction between maintenance operation and IS

| **Maintenance operation** | Maintenance operation |
|---|---|
| **Interaction on information Security** | |
| **Information** | Electronic information |
| **Risk** | Non-availability |
| **Threat** | Cut an electric wire |
| **Vulnerability** | External operator unattended |

The same example can be implicated to confidential documents on the desk and left. These interactions are defined either with specialized guides in the security or by domain experts.

We note that there is no work on ontology of interaction between the action to carry out a maintenance task and the consequences on information security this justifies the positioning of our problematic to implement a new model to represent the interaction between a task (operation) and maintenance of the ISMS information security management system.

# IV. ONTOLOGY (MISO) CONCEPTION & REALISATION

The ontology developed in our work named "Ontology Information Security & Maintenance (MISO)" is a task ontology.

In this conception, we used three different tools: StarUML[1] for the conceptualisation, Protégé 4.3[2] for the ontologization and NetBeans[3] for the operationalization, we resume in the figure bellow the different tools used for the conception of the ontology.

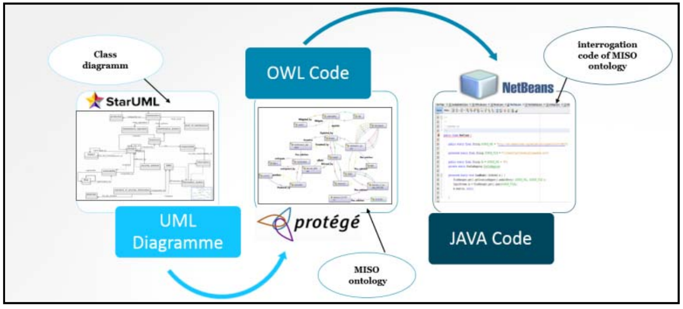


Fig. 3. The tools used for the conception of the Ontology MISO

Our approach is based on the UPON Lite method described and developed by De nicola & Missikoff, [19], on six stages divided into four categories for conceptualizing stage and the remaining two for ontologization (The figures.3). We completed our design

[1] StarUml is a UML tool by MKLAB http://staruml.io

[2] Protégé is a free opensource http://protege.stanford.edu/

[3] Netbeans is a software developpement plateform https://netbeans.org/

by another step "operationalizing" described in the book of Pierre Marquis et al [20].

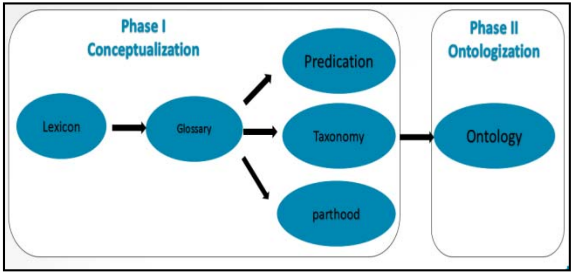


Fig.4. UPON Lite phases

The conceptualization is a description of the concepts and relationships in the real world. The stage of conceptualization result by a domain lexicon is represented in the table below:

Table [IV . concepts and relationships

| Concept | Relationship |
|---|---|
| Maintenance | Affected_by |
| Failure | threatens |
| Standard_of_security_in formation | Produce |
| Level_of_maintenance | Affects |
| Product | protecte |
| Impact | Respect |
| Control | Collect |
| Resources | Depends_on |
| Tangible_resource | Memorize |
| Machines | Is_the_responsability_of |
| ISO 2700x | PartOf |

The last step is to validate the model obtained in the preceding stage in collaboration with the expert in the field; the results are structured in a UML class diagram appointed using the StarUML tool in the figure below:

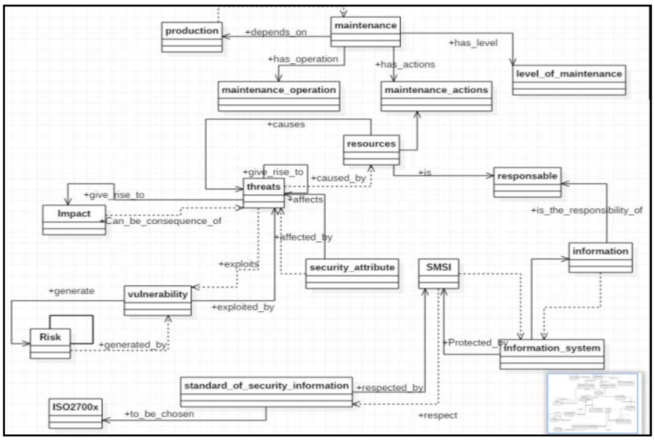


Fig.5. Diagram UML of the ontology MISO

The stage of ontologization result by the ontology "MISO" conceptualized by the tool "Protégé 4.3". The graph below is provided by the plugin "OntoGraph":

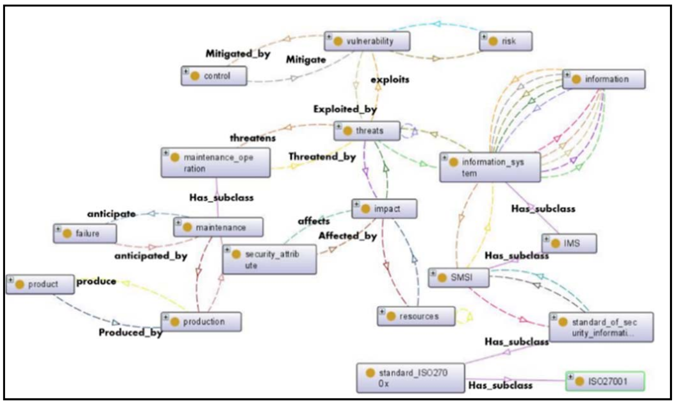


Fig. 6 . The ontology "MISO" in Protégé 4.3

## A. *The axioms:*

Description Logic (LDs) are decidable fragments of first-order logic for reasoning on axioms expressing logical constraints on unary and binary predicates. This is precisely what is required for reasoning with ontologies[20].

In our project we developped axioms, we define them in the table below:

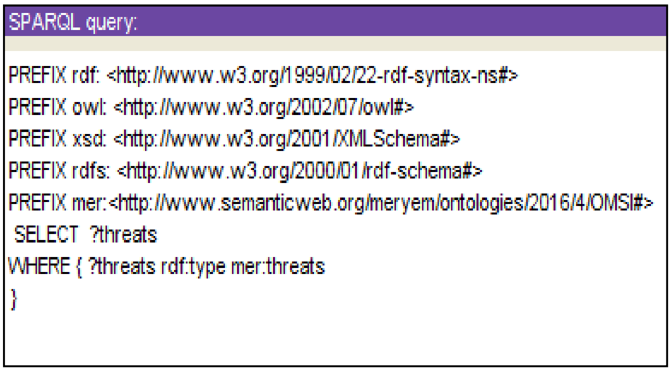
Table VI Axioms

| N | Concept | Logic expression |
|---|---|---|
| 1 | Maintenance | $\forall\, x\; Maintenance(x), \exists\, y\; level\ of\ maintenance\ (y) \rightarrow has\ level(x, y)$ |
| 2 | Threats | $\forall\, x\; Threats(x), \exists\, y\; risk\ (y) \rightarrow generate\ (x, y)$ |
| 3 | Maintenance operation | $\forall\, x\; Maintenance\ operation(x), \exists\, y\; human\ resources(y) \rightarrow executed\_by(x, y)$ |
| 4 | Subset | $\forall\, x\; subset\ \ (x), \exists\, y\; mode\ failure\ \ (y) \rightarrow has\ \ (x, y)$ |
| 5 | Vulnerability | $\forall\, x\; Vulnerability(x), \exists\, y\; threats\ (y) \rightarrow exploited\_by(x, y)$ |
| 6 | Control | $\forall\, x\; control\ (x), \exists\, y\; vulnerability\ (y) \rightarrow mitigate(x, y)$ |
| 7 | Information system | $\forall\, x\; information\ system(x), \exists\, y\; information\ (y) \rightarrow memorize\ (x, y)$ |
| 8 | SMSI | $\forall\, x\; SMSI\ (x), \exists\, y\; information\ system(y) \rightarrow secure\ (x, y)$ |
| 9 | Threats | $\forall\, x\; threats\ (x), \exists\, y\; maintenance\ operation\ (y) \rightarrow threatens\ (x, y)$ |
| 10 | Threats | ∀ x threats (x), ∃ y security attribute (y) → affects (x, y) |
| 11 | SMSI | ∀ x SMSI (x), ∃ y standard of security information (y) → respecting (x, y) |
| 12 | Impact | ∀ x Impact (x), ∃ y threats (y) → can be consequence of (x, y) |
| 13 | Machines | ∀ x machines (x), ∃ y maintenance (y) → maintained by (x, y) |
| 14 | Maintenance | ∀ x maintenance (x), ∃ y space part (y) → use (x, y) |
| 15 | Information | ∀ x information (x), ∃ y form (y) → is under (x, y) |
| 16 | Resources | ∀ x resources (x), ∃ y impact (y) → affected by (x, y) |

| | | |
|---|---|---|
| 17 | Resources | ∀ x resources (x), ∃ y threats (y) → affected by (x, y) |
| 18 | Threats | ∀ x threats (x), ∃ y security attribute (y) → affects (x, y) |
| 19 | Maintenance | ∀ x maintenance (x), ∃ y failure (y) → anticipate (x, y) |
| 20 | Responsible | ∀ x responsable (x), ∃ y threats (y) → causes (x, y) |
| 21 | Information system | ∀ x information system (x), ∃ y information (y) → collect (x, y) |

### B. *Request SPARQL:*

In this step of operationalization we used the tool of SPARQL query to extract knowledge from ontology "MISO" and JENA inference engine using NetBeans:

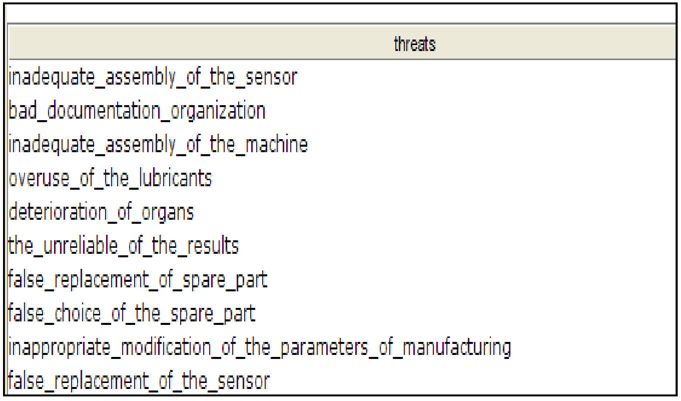


SPARQL query:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX mer:<http://www.semanticweb.org/meryem/ontologies/2016/4/OMSI#>
 SELECT  ?threats
WHERE { ?threats rdf:type mer:threats
}
```

Fig. 7. The request SPARQL

The result of the first request in our project is represented in the figure below:



| threats |
|---|
| inadequate_assembly_of_the_sensor |
| bad_documentation_organization |
| inadequate_assembly_of_the_machine |
| overuse_of_the_lubricants |
| deterioration_of_organs |
| the_unreliable_of_the_results |
| false_replacement_of_spare_part |
| false_choice_of_the_spare_part |
| inappropriate_modification_of_the_parameters_of_manufacturing |
| false_replacement_of_the_sensor |

Fig. 8. The result of request SPARQL

### C. *Sémantique Web Rule Langage (SWRL ):*

The next step in the semantic development value of ontology involves creating rules that convey more information about the concepts and their relationships. In fact, the wealth of a formal ontology depends on the level of detail included in the axiomatic definition of concepts and the number and diversity of rules encoded in the ontology.

- The first SWRL:

$$MaintenanceActions(?a), MaintenanceOperation(?o), Threats(?t), HasOperation(?a,?o), threatens\ (?t,?o) \rightarrow ThreatsAction\ (?t)$$

- The second SWRL :

$$MaintenanceActions(?a), MaintenanceOperation(?o), Threats(?t), Vulnerability\ (?V), HasOperation(?a,?o), threatens\ (?t,?o), exploits\ (?t,?V) \rightarrow VulnerabilityAction\ (?t)$$

### D. *The user interface :*

An interface that allows us to check the knowledge-defined concepts, their bodies and the links between them, this allows to provide relevant answers to queries and explore our Ontology, developed in Java, that allows providing relevant answers to queries. 3 choices: simple interrogation, it is a simple SPARQL Query, complex query that searches using more than one parameter value i.e. on two or more criteria. And the development button to develop the ontology by adding new items (not developed yet). The figure 9-shows the interface.

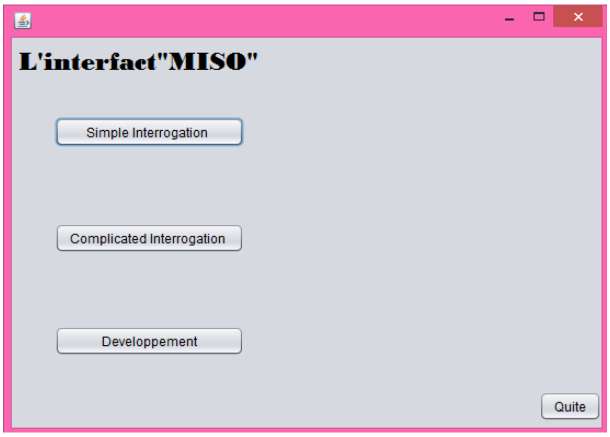


Fig.9. The interacts MISO

## V.Conclusion

This paper proposes a Maintenance Information Security Interaction Ontology; we have investigated the need to understand the requirements and attitudes towards security information that exist during a maintenance operation.

After research and establishment of the state of the art, UPON Lite method was used following its six steps.

We used StarUML for conceptualizing, Secure 4.3 for ontologization and for operationalization, the JENA inference engine in collaboration with NetBeans.
We developed an interface with java to make interrogation by SPARQL queries possible. It permitted the exploitation of the ontology and its instances for knowledge inference and decision making

The different tests showed that the proposed Ontology responds to a need of the operators of the two studied areas, In addition, we considered that MISO can efficiently determine the solution by using the interface to know what kind of risk or control is the best to choose.

For the perspectives of work, we propose an extension of the ontology taking into account more type of maintenance operations at different level, from 1 to 5.

Another research voice would be to develop a mathematical model based on extracted data from the ontology in other to resolve problems of optimisation.

ACKNOWLEDGMENT

I would like to pay special thankfulness, warmth and appreciation to the persons below who made our work successful and assisted us in different moments, M.Gouri M.Messikh M.Kaci M.Boudhar, for their support and assistance.

## References

[1] BEKKAOUI, M., KARRAY, M.-H., et SARI, Z. Knowledge formalization for experts' selection into a collaborative maintenance platform. IFAC-PapersOnLine, 2015, vol. 48, no 3, p. 1445-1450.

[2] Mohamed Hedi Karray, Brigitte Chebel-Morello & Noureddine Zerhouni, «A Formal Ontology for Industrial Maintenance », Terminology & Ontology : Theories and applications, TOTh Conference 2011., May 2011, Annecy, France.

[3] GRUBER T, « A translation approach to portable ontology specifications, Knowledge Acquisition », 1993.

[4] Neches, R, « « Enabling technology for knowledge sharing », 1991.

[5] « NF-EN-13306-X-60-319. Terminologie de la maintenance. Norme AFNOR.2001 ».

[6] Laallam F. Z., Sellami M., Gas Turbine Ontology for the Industrial Processes, "Journal of Computer Science", 2007, 3 (2), pp. 113-118.

[7] S. KLAI & Mohamed Tarek Khadi, « Ontology Construction and Evolution for a Steam Turbine Diagnostic Maintenance System », LabGED, Departement of Computer Science, University of Badji Mokhtar of Annaba, Algeria 2 Departement of Computer Science, University 20 Aout 55, Skikda, Algeria, 2009.

[8] F. ANGUEL, « Vers Un Système De Gestion Des Connaissances Pour L'aide Au Diagnostic De Pannes Dans Un Système Industriel », UNIVERSITE BADJI MOKHTAR -ANNABA, ANNBA-ALGER, 2003.

[9] Philipp Saalmann & al, « Application potentials for an ontology-based integration of intelligent maintenance systems and spare parts supply chain planning », Universität Münster (WWU), Leonardo-Campus 3, 48149 Münster, Germany, 2015.

[10] Hassen Turki « Développement d'un outil d'aide à la gestion de la sécurité dans les réseaux TCP/IP : SATAN » Projet de fin d'étude filière ingénieur en télécommunications- SUP'COM promotion 2005.

[11] Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing 1(1), 11–33 2004

[12] SI AHMED Boualem, « Le management de la sécurité : norme Iso 27001 », Ecole Nationale Polytechnique, Département de Génie Industriel, 2009.

[13] Heinz-Peter Berg, «Risk Management: Procedures, Methods and experiences »,Bundesamt für Strahlenschutz, Salzgitter, Germany,2010.

[14] B.Barthélémy, J.Quibel Gestion des risques de l'entreprise, 2000.

[15] Tung Ju Chiang, Shiang Kouh, et Ray-I Chang, « ISO 27006 : Exigences pour les organismes réalisant l'audit et la certification de SMSI, mis à jour Vendredi, 22 Janvier 2016 12:30 », IJCSNS International Journal of Computer Science and Network Security, 11-nov-2009.

[16] Thomas Neubauer, Andreas Ekelhart, & Stefan Fenz, « Ontology-based Generation of IT Security Metric ».

[17] Tung Ju Chiang, Shiang Kouh, et Ray-I Chang, « ISO 27006 : Exigences pour les organismes réalisant l'audit et la certification de SMSI, mis à jour Vendredi, 22 Janvier 2016 12:30 », IJCSNS International Journal of Computer Science and Network Security, 11-nov-2009.

[18] Amina Souag, Camille Salinesi, & Isabelle Wattiau, « Ontologies for Security Requirements: A Literature », University Paris 1, France, 2009.

[19] ANTONIO DE NICOLA & MICHELE MISSIKOFF, « A Lightweight Methodology for Rapid Ontology Engineering ».

[20] Pierre Marquis, Odile Papini, et Henri Prade, Représentation des connaissances et formalisation des raisonnements, CEPADUES. Toulouse-France,2014.