Master research Internship

Bibliographic report

Analysis and prevention of security risks in industrial systems of the future

Domain: Modeling and Simulation - Cryptography and Security

Author:
Idris TSAFACK TANKEU

Supervisor:
Laurent NANA
David Espes, Sophie Gire,
François Monin
SFIIS Lab-STICC

Abstract: Increasingly, humans challenge the laws of nature by integrating technological aspects at all levels (industries, construction, transport, medicine, social life, etc.). These incessant technological innovations, which are considered to be an advance of the human species, do not only provide services more and more important to our live experience, but also systems whose insecurity would be fatal.
In this document, we present the different network security challenges facing industrial systems of the future and we explain some risks analysis and prevention methods in industrial systems, through the study of security models such as attack graphs via its TVA[1] approach, petri nets, formal models, Bayesian and Monte Carlo approaches. In addition to defining a team risk analysis approach in the industrial context, we present a use case where we show how formal methods can be used to build a secure industrial system through known vulnerabilities from public databases.

Contents

1 Introduction **1**

2 Statement of Problem **1**

3 Overview of safety, reliability and security in industrial systems **2**
3.1 General context to risk and safety analysis activity 2
3.2 Typology of network security methods 3
3.3 Issues associated with static and dynamic security models 4
3.4 Some strengths and weaknesses of secutity analysis methods 5
3.5 New security challenges in industrial systems of the future related to cyber defense . 6

4 Approaches for risk prevention and security in industrial systems **7**
4.1 An approach for risks analysis relating to industrial installations 7
4.2 Static method by attack graphs and Topological Vulnerability Analysis (TVA) approach 8
4.2.1 Problems to be solved by attack graphs 8
4.2.2 Construction of attack graphs via the Topological Vulnerability Analysis (TVA) approach 8
4.3 Dynamic secutity method by Petri Nets 9
4.4 A bonus to security models with the Monte Carlo method and the Bayesian approach 10
4.4.1 Dynamic security method by Monte Carlo approach 10
4.4.2 Dynamic security method by Bayesian approach 11
4.5 Use case: detection of attacks based on known vulnerabilities in industrial networked systems via formal methods 11
4.5.1 Presentation of the security method 11
4.5.2 Formal model and prototype implementation 12

5 Conclusion and perspectives **13**

[1] Topological Vulnerability Analysis

1 Introduction

The current context of the evolution of technology is such that any industrial system that wants to be scalable, efficient, secure and competitive can not succeed without taking into account the new advantages brought by the IT Networks and the Information and Communication Technologies. It is worth noting that these waves of new technologies are emerging with the batch of security risk **(see [5])** that goes along with. Vulnerabilities in industrial software and hardware components can be exploited by attackers to cause damages through the cyberspace which abounds several types of hackers. This is one of the fundamental reasons why the safety of industrial systems has become an indispensable pillar of scientific research on network security.

Managing risk is an iterative process that aims to identify, analyze and minimize risk or keep it within acceptable limits. The analysis and prevention of security risks is a key step in the risk management process and ensures greater operational reliability of systems. In order to succeed in this analysis activity, we have to implement a model that faithfully represents the behavior of the industrial system studied. The elements used to model the behavior of a system are various and varied **(see [29])** : diagrams, trees, specific models, networks, behavior description languages, spreadsheets, etc. Whatever the solution used to model the behavior of an industrial system in order to determine the security risks, it must provide a model capable of accurately reproducing the behavior of the system when it evolves over time by being subjected to various hazards such as insecurity, failures, repairs, tests, procedures, external events, etc. Therefore, the principal purpose of our research work at Lab-STICC will be to propose methods and security models for risk analysis.

This paper is organized as follows : first, we present clearly the problem posed by the research topic (section 2), then comes the state of the art (Section 3) on the general context **(see [29])** to risk and safety analysis activity. Once the new challenges confronting industrial systems in the cyber security world **(see [25])** have been illustrated, we will present (Section 4) a reliable approach for risk prevention **(see [6])**, followed by models of risk prevention by the sureness of operation then some static and dynamic safety models **(see [11, 9, 25, 24, 28, 36])** proposed by other research work. Finally, before concluding (Section 6), we will discuss the results (Section 5) and the impact that the proposed methods have on the problem stated.

2 Statement of Problem

Industrial systems of the future will include a significant share of new technologies information and communication networks (networks, new communication interfaces, softwares, etc.), leading to security problems that are currently non-existent. It is essential to anticipate these problems in order to ensure the proper functioning of the next-generation industrial systems which will no doubt be confronted with the increase in the attacks and malicious acts observed to date at different levels. The security of industrial systems **(see [5, 6])** is today mainly centered on the hardware part, the software part being less important, and the networks used are very often less open and therefore less vulnerable. However, various forms of attacks that can have very serious consequences on the operation of industrial systems exist in communications networks, web-based software and technologies. New web technologies face several forms of threats, including : (1) **Sniffing** passwords and packets; (2)**IP spoofing** : the hacker's computer can pretend to be a known computer; (3) **Scanners** : which let you know which ports are open on a given machine; (4)**Trojan horses** : program that hides itself in another program apparently above suspicion; (5)**Worms** : a program

capable of propagating and self-reproducing without the use of any program or action by a person; (6)**Traps** : an entry point into a computer system that goes above normal security measures; (7)**Logic bombs** : programmed devices that are triggered at a specified time by evaluating the system date, launching a command, or any call to the system; (8)**The Flood** consists in sending rapidly packets of information to the router machine, which may cause the machine to crash; We will not cite the set of threats or vulnerabilities existing on the web, but we specify that there are many others.

One of the objectives of this research work is to study the impact of the contribution of new technologies on the safety of industrial systems, as well as the means to secure the industrial systems integrating these technologies. Most of the security properties of systems, whether software or hardware, can be translated by graph properties **(see [7, 17])**. Also, the approach recommended in this research work is to compare the different types of security models**(see [11, 36, 24, 38, 26])**, whether static or dynamic. For the static approach, the most commonly used method is the attack graph **(see [11, 37, 28, 36])**. As regards the dynamic method, Petri nets **(see [24, 38])** are one of the most widely used approaches. Therefore the overall research work will be carried out in several phases: (1)State of the art on the use of safety models; (2)Study of the special case of industrial systems; (3)Comparison of different models within these systems.

The industrial networks of the future will integrate in their architectures the hardware or software tools used in computer networks, these components being generally vulnerable to the threats listed above. It is therefore time to put in place security models to prevent the risks involved. In summary our research work aims to study and propose solutions for the analysis and prevention of security risks in industrial systems of the future, based on the use of security models. It is proposed within the framework of the activities of the SFIIS team of the CID cluster of Lab-STICC.

3 Overview of safety, reliability and security in industrial systems

By placing the risk analysis in its general industrial context, this section first presents the state of the art relating to our research topic and then defines the main concepts related to risk and its analysis. In addition, there is a synthesis of the different existing approaches: internal methods including physical and functional modeling, external methods including statistical and expert approaches. Then we show the main differences between static security model and dynamic safety model, then we'll finish on new security challenges faced by industrial systems of the future.

3.1 General context to risk and safety analysis activity

The concept of risk has a large number of meanings and confusion is often made with the concept of probability, whether in common languages or in technical references. Nevertheless, in the industrial context, there is a clear consensus on the definition of risk, which aims to associate two entities from which it is more generally defined: probability and consequence **(see [3, 27])**. We prefer to retain a more general definition proposed by Villemeur **(see [4])** which has the advantage of not taking into account only the probabilistic approaches of risk analysis: **"risk is a measure of a hazard involving a measure of the occurrence of an undesirable event and a measure of its effects or consequences"**. The risk analysis activity logically consists of answering the following 3 questions **(see [35])** :

- **What can lead to situations of danger?** : search for **"Si"** scenarios that may lead to a failure;
- **What are the chances for these risk situations to occur?** : evaluation of the possibility of occurrence of each; scenario "Si" from a measure of occurrence **"Pi"**;
- **If they occur, what consequences should be expected ?** : describe and estimate the **"Ci"** consequences of the "Si" scenario.

Therefore, a risk **R** is defined by the triplet **(see [27])** : $R =< Si, Pi, Ci >$

There are several approaches to performing risk analysis and prevention activities, which are clearly identified and formalized in the industry sector. They can be grouped into two families **(see [1])** : internal methods and external methods of risk analysis.

Internal methods rely on deep knowledge of the functioning of the system under study (a set of interconnected components in the industry), based on modeling, it is then possible to predict its future behavior and then analyze the risks. Depending on the type of model describing the system, there are two approaches to modeling internal methods: (1) **Physical modeling** which takes into account the equations governing internal phenomena. (2) **Functional modeling by Safety of operation**: here we design models to determine the interactions between the components of a system and its environment, so as to establish in a formal way the links between the failures or vulnerabilities of components, their causes and their effects.

External methods are applied in contexts where the modeling of physical or functional mechanisms is technically not possible or not adapted to the level of concern. There are two approaches to analysis relating to external methods: (1) **Approach by statistics** which requires a rich and well documented feedback of experience. (2) **Expertise approach** (where the human expert is the only person capable of predicting the evolution of a system).

3.2 Typology of network security methods

Before carrying out a risk analysis, it is essential to analyze the system to be studied. This analysis is based on a model that faithfully characterizes the behavior of the system under study (SUD). Models can be built using several types of risk analysis methods. There are different classifications of risk analysis methods **(see [29])**. During our research, three of these classifications have attracted our attention.

A) **Quantitative or Qualitative** : a qualitative risk analysis approach consists of identifying not only dangerous events or the sequence of hazardous events (scenarios) that may lead to a risky situation but also the causes and consequences of these events. While a quantitative method consists in numerically characterizing the system to be analyzed, for example determining the failure rate, the probability of occurrence of a failure, the costs of the consequences, etc. At present, qualitative reasoning makes it possible to fill in some of the inadequacies of numerical methods in fields where knowledge is not formalized or difficult to quantify; It comes in addition to quantitative reasoning.

B) **Inductive or Deductive** : inductive diagnostic methods correspond to a "rising" approach where all possible combinations of elementary events can be identified, which can lead to a single undesirable event: failure or exploitation of vulnerability. For deductive methods, the approach is reversed since one starts from the undesirable event, the failure or potential exploitation of vulnerability, and then a top-down approach is sought for all possible causes.

C) **Static or Dynamic** : a dynamic method allows to take into account the evolution of the configuration of the components of the system over time, whereas a static method studies a

system at different times of its life cycle, that is to say for different States, without being interested in the transitions between these states.

3.3 Issues associated with static and dynamic security models

Here we present the differences between static and dynamic security methods, as well as the impact on analysis and risk prevention on the industrial system studied. In the classification of the methods, we will insist on static and dynamic methods. Indeed, these two methods characterize the nature of the relationship between the security model of the system and the operation of the system modeled in relation to its topology.

When a **static method** is used, then the risk analysis performed with the corresponding security model is reliable as long as the network architecture (industrial or IT[2]) does not change. As an example of a change in the architecture of the network we can mention: the addition or removal of a network equipment (router, server, etc.), software (antivirus for example), the modification of the rules of a firewall, updating some network components that cause the addition, modification, or removal of certain vulnerabilities. In this static context, one of the most used security models is the attack graph **(see [28, 37, 36])**.

Dynamic methods as opposed to static security methods, take into account the fact that the architecture (topology) of the network can change during its operation, in this case the model proposed for the risk analysis will automatically adapt to the new network parameters, leading to an update of the risk analysis previously carried out. In this dynamic context one of the most used security models is the petri net **(see [24, 38])**.

Static and dynamic risk analysis methods identify hazardous events or the sequence of hazardous events (scenarios) that can lead to a risky situation, the causes, the consequences of these events. Depending on the concepts we define regarding whether a method is static or dynamic, we can classify some of the security methods identified during our research.
Below we cite some static security methods, that is to say that provide models whose modification of the topology of the studied system, will lead to a reanalysis of the security risks :

- Attack graphs method : static and inductive, we will detail this method in section 4;
- State Space (MEE) Method: quantitative, inductive;
- Method of the diagram of success or Reliability: quantitative, inductive;
- Fault Tree Method (MAD): quantitative and deductive;
- Consequence Tree Method (MACQ) quantitative, inductive;
- Preliminary Risk Analysis (RPA): quantitative and deductive;
- Method of combinations of failures summary: quantitative, deductive.

Apart from the method by the attack graphs, the other static methods that we have just mentioned are most used in the context of the reliability of operation, these methods are studied with examples supported by H. Niandou, A. Talon, D. Boissier and L. Peyras **(see [29])**. The reliability of functioning **(see [4])** is very important in the field of analysis and prevention of risks.
We can cite the following dynamic methods:

- Petri nets: quantitative, inductive;
- Markov processes: quantitative, inductive;
- Stochastic Game Theory.

[2]Information Technology

Some methods can be used in conjunction with the above-mentioned methods in static and dynamic contexts. Some of them are :

- Monte Carlo method (quantitative);
- Temporal analysis (qualitative);
- Formal methods.

We will give more clarity about the Petri nets and Monte Carlo method in Section 4. We will also present a case study where we show how to construct an attack graph (based on known vulnerabilities) **(see [11])** via modeling the operation of an industrial network by formal methods.

3.4 Some strengths and weaknesses of secutity analysis methods

The preceding sections have not presented the advantages and limitations associated with each of the risk analysis methods, here we propose a global synthesis **(see [11])[6])**. We mention the benefits below.

A) **Systematic nature**: The first advantage of risk analysis methods lies in their systematic nature. Indeed, they allow to envisage in a methodical way, the different situations of danger and events feared as well as their causes and consequences. This systematic aspect is particularly important in order to identify hazards in the most exhaustive manner possible. Moreover, these methods enable technical elements to be provided to judge the control of risks at the source, thanks in particular to the identification of existing security barriers or to considering the risks in question. This risk control can only be demonstrated if all the possible causes and consequences are considered. In the case of an industrial site, this work can be complex and these methods thus constitute a valuable aid in guiding reflection.

B) **Complementarity of methods**: as mentioned above, these methods of risk analysis are generally complementary. This makes it possible to retain the tools most adapted to the particular case to be treated and to be able to ensure an in-depth analysis of an industry using tools that are increasingly dedicated to well-defined parts of this system.

C) **Exchange and communication tools**: Most risk analysis methods are fully effective when implemented in a multidisciplinary working group. As such, they are a tool for exchange and communication between people of different sensibilities and professions. Thus, the richness of these methods is found not only in their basic principles, but also in the experience gathered within this working group. The meetings thus lead to the sharing of various experiences and to reflect in a global and realistic way on the safety of the installation under consideration.

Opting for methods to perform the risk analysis does not only provide benefits. We cite three main limitations inherent in the traditional methods of risk analysis.

A) **Risks of external aggression**: although the methods presented may consider the possibility of external aggressions affecting the installation studied, they are mainly dedicated to the identification of risks generated by this installation on its environment. In other words, it is essential to carry out a phase of identification of the sources of external aggressions as associated with the possibility of domino effects, climatic or environmental conditions (lightning, earthquakes, etc.) or acts of malevolence.

B) **Risk estimation**: risk analysis methods allow the working group to estimate risks in terms of likelihood and severity. In terms of risk analysis, this risk assessment is carried out in a simplified way and should not be considered as an accurate assessment tool. A more accurate assessment of severity may remain essential for the most critical risks.

C) **Not exhaustive**: the use of risk analysis methods such as those presented in this document is a valuable aid in the identification of risks but does not guarantee 100% that all the accidents likely to occur have been identified. The exhaustiveness depends on the experience gained in the working group and the time and resources devoted to the analysis.

3.5 New security challenges in industrial systems of the future related to cyber defense

The industrial networks of the future, meaning networks which will change their hardware and software infrastructures to new technologies (most of which incorporate functionalities relating to the web and IT networks), will also have to evolve their security mechanisms so that new threats engendered should be analyzed and prevented. Therefore, industrial systems of the future will have to include security mechanisms associated with cyber-security (IT networks) in their systems. The cyber security mechanisms to be implemented by the industrial systems of the future must be the most up-to-date and the most adapted to their contexts. Therefore, these mechanisms will have to deal with security issues related to cyber security. In the cyber security universe, there are various security issues **(see [25])** that industrial systems will have to consider.

Nowadays, cyber defense, which corresponds to the dynamic and real-time aspects of computer security in order to be able to detect attacks and defend oneself, is based on a variety of security tools and products such as Intrusion Detection Systems (IDS), vulnerability scanning tools, antivirus, and systems for management and correlation security events (SIEM[3]). These tools, although very effective each in their field, produce a lot of highly technical information, which often requires experts to be able to analyze and exploit all their results. Moreover, most of these tools have not been designed to be interoperable, and their results are often only intended to be read and analyzed by a human operator. When it comes to supervising a large-scale computer system spread across multiple sites, it becomes very difficult to correlate and analyze all available sources of information in **real time** to detect anomalies and incidents Fast enough to react effectively. This complexity is due to the amount of information generated, as well as the heterogeneity of the formats used.

Another weakness of current security products in cyber space is the visualization of this information: for example even the most costly vulnerability and event correlation tools are not yet able to visualize accurately their results on a map of the network. To provide an overview of the situation. There are now a growing number of tools that can be used in cyber defense for visualization **(see [2, 33])**, but these are for the most part intended to graphically analyze the network traffic or a large number Events to detect anomalies or trends. The use of visualization to obtain a view (Vulnerabilities, alerts, incidents) is still poorly developed.

A third major problem in cyber defense is that each detection or monitoring tool provides only partial and relatively low-level results for the IT and network infrastructure (it will be idem for industrial network). The task of understanding the actual impact of an IDS[4] vulnerability or alert is typically devolved to a human analyst, who must himself link all technical information to his knowledge of all services or processes that depend on the related network components. It is therefore necessary to develop new tools for dynamic risk analysis, with a more comprehensive view of the problem. In order to address these gaps the purpose of the CIAP and DRA projects in the NATO C3 Agency explore **(see [25])** possible solutions.

[3]Security Information and Events Managemen

[4]Intrusion Detection Systems

Since threats, vulnerabilities and configurations are continually evolving in information systems and computer network (will be idem for industrial network of the future), it is very difficult to carry out a risk analysis at any given time, ensuring that the results will always be valid for the medium and long term. Therefore industrial systems of the future will have to use dynamic security models to provide a real-time risk analysis, and determine automatically the actual impact due to the overall security situation of the system and network. The global solution proposed should also be able to automatically recommend possible responses to reduce the risks that have increased.

4 Approaches for risk prevention and security in industrial systems

In this section we begin by presenting an approach **(see [6])** that allows to situate the security models in a global procedure of analysis and prevention of risks, then we will talk about the use of attack graphs as a static model of security and its TVA[5] approach **(see [22])**. Furthermore we will present succinctly the dynamic method of risk analysis by the Petri nets **(see [29])**, then we will show the interest of using the Bayesian **(see [32])** and Monte Carlo **(see [29])** methods in the analysis of the security risks, finally we will briefly present a use case where we will discuss about a static security model that characterizes an industrial system by a formal model in order to construct graphs of attacks based on known vulnerabilities **(see [11])**.

4.1 An approach for risks analysis relating to industrial installations

The following paragraphs present an approach used to analyze and prevent security risks associated with the operation of industries. This process is usually broken down into several stages **(see [6])**.

Definition of the system to be studied and the objectives to be achieved: this preliminary step makes it possible to define clearly the framework of the risk analysis, the criteria of analysis and the conditions of acceptability of risk. For example, it may be necessary to carry out a risk analysis in order to analyze more specifically the risks related to the operation of the industrial network.

Collection of information required for analysis : before starting the procedure, it is generally necessary to follow the following steps: functional and technical description of the system (identifying the functions of the system studied, characterizing the structure and the operating conditions of the system, ...), description of its environment, identification of potential internal and external hazards, analysis of past incidents/accidents.

Definition of the approach to be implemented : here, it is a question of choosing the most appropriate method of risk analysis among a large number of tools or methods dedicated to safety. The choice of the right model of safety is essential to the success of the entire analysis work.

Implementation of risk analysis in working groups : the people in the working group are chosen for their skills (knowledge and experience) in specific technical fields. They are not necessarily familiar with the use of risk analysis and prevention tools. The objective of the group will be to consider in the most exhaustive way all the risks generated by relying on safety models.

[5]Topological Vulnerability Analysis

4.2 Static method by attack graphs and Topological Vulnerability Analysis (TVA) approach

4.2.1 Problems to be solved by attack graphs

Cyber security is inherently difficult. Protocols are often insecure, software is frequently vulnerable, and educating end-users is time-consuming. Security is labor-intensive, requires specialized knowledge, and is error prone because of the complexity and frequent changes in network configurations and security-related data. Network administrators and security analysts can easily become overwhelmed and reduced to simply reacting to security events. A much more proactive stance is needed. Furthermore, the correct priorities need to be set for concentrating efforts to secure the network. Administrators and analysts often have a vertical view of the particular component they are managing; horizontal views across/through the infrastructure are missing. This in turn shifts emphasis to vulnerabilities at the interfaces. Security concerns in a network are also highly interdependent, i.e., susceptibility to attack can depend on multiple vulnerabilities across the network. Attackers can combine such vulnerabilities to incrementally penetrate a network and compromise critical systems.

However, traditional security tools are generally point solutions that provide only a small part of the picture (entire network). They give few clues as to how attackers might exploit combinations of vulnerabilities to advance an attack on a network. It remains a painful exercise to combine results from multiple tools and data sources to understand one's true vulnerability against sophisticated multi-step attacks. It can be difficult even for experienced analysts to recognize such risks, and it is especially challenging for large dynamically evolving networks. The innovative approach to proactive cyber security through attack graphs is commonly referred to as Topological Vulnerability Analysis (TVA).

4.2.2 Construction of attack graphs via the Topological Vulnerability Analysis (TVA) approach

Attack graphs make it possible to map all paths across the IS[6] while providing a "deep" defense capability, with multiple mitigation options, rather than rely solely on the usual defenses of the IS (eg firewall). The TVA[7] approach **(see [28])** breaks down the generation of attack graphs into two phases: 1 / capturing an SI model, and 2 / using the model to simulate the penetration of the IS via several steps. This model contains the configuration of the IS and the exploits[8] of known attackers. In attack simulation, the input model is analyzed to form a graph of attack exploits according to the constraints specified by the user. The TVA approach is based on the topological modeling of the IS, its security conditions (analysis of known vulnerabilities **see [13, 20, 14, 31, 15, 16]**, and knowledge of exploits by potential attackers. Traditional approaches dealing only with IS data and security events, regardless of the context provided by the attack graphs, are clearly insufficient. The representation of combinations of IS attacks in the form of graphs via the TVA approach offers enormous advantages. **The TVA consists of combining the vulnerabilities in the manner of a real attacker, discovering step by step all the paths of attack through an SI, considering the exhaustiveness of the data used to construct the graph.** To define these graphs, we analyze the inter-dependencies between vulnerabilities and construct

[6] Information System
[7] Topological Vulnerability Analysis
[8] exploiting vulnerabilities

a complete map indicating all the possible paths, direct or in several stages, of an IS. "TVA" requires modeling IS (idem for the industrial network) components, including applications, their vulnerabilities, and connectivity/dependencies to the processes/services at stake within the IS. It then compares the configuration of the IS with a database of exploits modeled in order to simulate the course of chained attacks. The resulting attack graph thus allows to map all the possible ways of exploiting vulnerabilities, showing how attackers can get into the IS and what processes and resources they might compromise. The attack graphs obtained provide the context for coping with intrusion attempts. This includes tips for deploying and configuring Intrusion Detection Systems (IDS probes), correlating intrusion alarms, and predicting possible next attack steps. For example, the attack graph can guide the placement of intrusion detection probes to cover critical attack paths (such as those leading to unavailability of critical services), while minimizing redundancy. Another advantage of attack graphs is that they can allow the filtering of false alarms (noise reduction due to irrelevant safety events), based on known paths of residual vulnerabilities. However a constraint of the TVA approach lies in the need to keep attack graphs up to date with changes to the SI (configuration, vulnerabilities, ...) in order to present a situation faithful to the current state of the attack paths.

Even today, attack graphs of this type are often created manually by "security" teams (architects security, penetration testers, ...). Several works such as the Technical report published by the George Mason University **(see [23])**, have demonstrated the use of computational capabilities for the generation of attack graphs, rather than relying on a tedious, non-exhaustive and often error-prone manual creation. Several software tools can be used to automatically generate attack graphs from a knowledge base containing logical facts and rules and to implement other features of the TVA approach. We can cite: SlyBox, NetSPA, **Mulval**: uses the Datalog language, a derivative of Prolog, to express these facts and rules; **AssetRank**: a tool developed by Defense Research and Development Canada (DRDC) to add metrics to the results of MulVAL, so as to prioritize them and highlight the most critical nodes of the attack graph. The algorithm of AssetRank is inspired by PageRank, used by Google to sort the results of its search engine based on priorities. AssetRank makes it possible to identify which attack paths are most likely from the point of view of the attacker according to various criteria (ease of operation, stealth, criticality of the targets, etc.). As an example of a project using MulVal and AssetRank, we can mention two research and development projects of the NATO NC3A agency in the field of cyber defense **(see [25])** : CIAP (Consolidated Information Assurance Picture) and DRA (Dynamic Risk Assessment).

4.3 Dynamic secutity method by Petri Nets

Petri nets make it possible to represent a dynamic safety model, developed to handle dynamic systems. Meaning that they allow to model systems whose architecture can change at any time (addition/withdrawal of a network equipment, installation of software, update of firewall, ...). These systems pass from state to state at the end of random durations governed by various phenomena (components failure, repairs, external events, testing, etc.) to which it is subjected (stochastic behavior). During its evolution, the Petri network sequentially traverses the different states of the modeled system.

A Petri net can be used to: (1 Analyze in detail the sequential behavior of the system, (2)Identify the states for realization of a state graph, (3)Search for inaccessible states in a graph, (4)Search for deadlocks, causes of waiting, closures, search for effective conflicts (situations where several transitions having a common input place are valid at the same time, but not all of them can be

fired successively). The use of Petri networks to identify the various states of the system in order to generate the equivalent Markov process is one of the most common applications in the context of safety and reliability. A Petri net is an oriented graph whose vertices can be either places

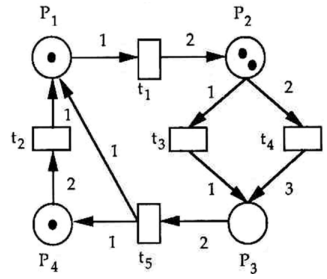

Figure 1: An example of Petri net

(represented by circles) or transitions (represented by rectangles). The vertices of a Petri net are connected by arcs. An oriented arc always connects two vertices of different natures. The dynamic aspect, in a Petri net, results in the presence of tokens represented by points.

Although the number of states generated by a Petri net is countable, it is not necessarily finite. As soon as the system studied is complex, the number of states generated is important and it is no longer possible to identify them all. The graph corresponding to the Petri network can be large so as to be difficult to analyze. Sometimes we may have to analyze a particular process (critical scenario) in detail. For this purpose the Petri net method can be used together with the Markov processes method. Using the Markov method, we associate a transition rate with each transition of the process studied. This Petri net method can only be used to generate a Markov graph when the number of states is not too large (up to a few thousand).

4.4 A bonus to security models with the Monte Carlo method and the Bayesian approach

4.4.1 Dynamic security method by Monte Carlo approach

The method of Monte Carlo and the Bayesian method are other methods used in the context of security analysis. The objective of the Monte Carlo process is to model finely the behavior of a complex system passing from state to state after random durations governed by various phenomena to which it is subjected (stochastic behavior). The behavior patterns (security models) of systems are diverse and varied: diagrams, trees, attack graph, Petri nets, behavior description languages, formal models, etc. In order for the Monte Carlo method to be reliable, these other models must be capable of reproducing in a sufficiently realistic way the behavior of the system when it evolves over time by being subjected to different hazards. It can thus be seen that the Monte Carlo method alone is of little use. It is coupled with a method of modeling (static/dynamic) in order to study finely a random process, generally when the Markov method is inadequate (due to the fact that transition rates from one state to another are random, in the case of a model described by a graph).

Relating to the Monte Carlo method, a **Story** (or trajectory) is one of the possible evolution of the system with its failures, its repairs, etc., over a defined duration. Once the first story is generated, the Monte Carlo method will also generate a second story that represents another possible evolution, then a third, and so on. In each of them, the parameters of interest (passage or

residence time in certain states, number of occurrences of an event, costs, etc.) are recorded so as to constitute statistical samples. The Monte Carlo simulation is a very interesting method because it gives access to many parameters inaccessible by other methods and leads to extremely detailed analyzes of the studied systems.

There are several advantages to using this method in particular: (1)The increase in the power of the computer means makes it easy to apply this method, (2)It is not limited by the number of states of the system studied because, even if there are hundreds of thousands, only the preponderant states appear during the simulation, (3)It allows the taking into account of any law of probability, (4)It allows the association in the same model of deterministic phenomena and random phenomena, (5)Its IT implementation is easy. However, there are some disadvantages including: (1)The stochastic dependence of the data, (2)The number of stories to be realized: the fewer events required, the greater the number of stories needed.

4.4.2 Dynamic security method by Bayesian approach

A number of researchers have proposed risk assessment methods by building security models of network systems, using paradigms like attack graphs and attack trees **(see [19, 34])**, and then finding attack paths in these models to determine scenarios that could lead to damage. However, a majority of these models fail to consider the attacker's capabilities and, consequently, the likelihood of a particular attack being executed. These risk models do not help reason about the causal dependencies between network states, the optimization formulations ignore the issue of resource availability while analyzing a risk model. Without these considerations, threats and their impact can be easily misjudged. To alleviate such drawbacks, Dantu and al. **(see [18])** propose a probabilistic model to assess network risks, they model network vulnerabilities using attack graphs and apply Bayesian logic to perform risk analysis. Nayot Poolsappasit and al. **(see [32])**, propose a risk management framework using Bayesian networks that enable a system administrator to quantify the chances of network compromise at various levels. They also show how to use this information to develop a security mitigation and management plan.

4.5 Use case: detection of attacks based on known vulnerabilities in industrial networked systems via formal methods

4.5.1 Presentation of the security method

Through a case study, we present the design of a formal model and the development of an automated analyzer (software tool) that can assist in the design and maintenance of an industrial network when security is considered. This work by Manuel Cheminod et al. **(see [11])** shows us how to use formal models to describe the functioning of the system, and formally describe the known vulnerabilities that can be exploited in the network, to finally generate an attack graph. Known software vulnerabilities are collected **see [13, 20, 14, 31, 15, 16]**, sorted and updated in public databases (OSVDB, Symantec, Siemens AG, ICS-CERT, etc.) for several years. The main interest of this method is to match the vulnerability analysis and the verification of access control policies within the industrial network. The main objective is to highlight the possible paths of attack, exploiting the vulnerability chains, constituting a threat to the system security. The proposed model also includes elements for extending security to the centralized authentication mechanisms commonly used in modern IT systems (Microsoft Windows Active Directory, Apache Central Authentication Service, etc.).

4.5.2 Formal model and prototype implementation

The system implementation view consists of a data model D: describing all the objects of the system and their physical and/or logical interconnections, the initial state for each user considered (i.e. the physical location, the credentials held, etc.), a set of inference rules that govern interactions between users and the system. It should be noted that the data model D is system-specific and must be provided by the designer, while the set of inference rules is predefined and fixed by the security method (will be integrated to the core of the software). We consider the system to be static, meaning that we assume that the interactions between the users and the system do not affect the description of the system D. This assumption is not restrictive, it can be taken into account by modifying the data model D offline and consequently re-performing the compilation of the model on the software tool (analyzer).

Formally, the security model D is defined as follows:

$$D ::= (\Omega, \Lambda) \tag{1}$$

$$\Omega ::= \omega^* \tag{2}$$

$$\Lambda ::= \lambda \tag{3}$$

Eq.(1) defines the industrial system, Eq.(2) defines all the objects of the system, meaning entities on which Operations can be carried out. Objects include parts (e.g: a server room) and other physical containers (cabinets, etc.), servers (web, databases, messaging), applications and networking devices (firewalls, switches, routers). And Eq.(3) defines a set of physical communication links.
Object definition :

$$\omega^* ::= \langle \omega_{id}, \{\pi^*\}, \omega_{path}, \{acc\}, \{pp\}, \{fr\}, \{sw\} \rangle \tag{4}$$

$$\pi^* ::= \langle \pi, \{\langle d, \{c\} \rangle\} \rangle \tag{5}$$

$$\pi^* ::= \langle \pi, \{f\} \rangle \tag{6}$$

Eq.(4) defines any object $\omega \in \Omega$ in the system D where ω_{id} and ω_{path} are the object identifier and path-name, respectively. Indeed, in the data model objects can be nested (i.e., an object can contain and can be contained in other objects, so as to allow, for instance, the description of virtual hosts within hypervisors) and anyone of them is uniquely identified by both its identifier and its path $\omega_{path} = \omega_{id1}, \omega_{id2}, ..., \omega_{idk}$. Any object ω includes a set of operations ($\{\pi^*\}$ in Eq.(4)) representing all possible actions a user may, in principle, carry out on the object itself. The object formal description is given below:

f ::= $pre, post$
pre ::= $\langle phy\_acc\,[c] \rangle$
| $\langle loc\_acc\ \omega' : n'\,[c] \rangle$
| $\langle loc\_acc\ \omega' : g'\,[c] \rangle$
| $\langle rem\_acc\ port\,[c] \rangle$
| $\langle rem\_auth\ lp\,[c] \rangle$
| $\langle phy\_acc \wedge auth\ \omega_{aa} : n_{aa} \rangle$
| $\langle rem\_acc\ lp \wedge auth\ \omega_{aa} : n_{aa} \rangle$

$port$ ::= $dla | lp$
lp ::= $\langle id_{lp}, [pn], na, [pr] \rangle$
$post$ ::= $[\omega'' : n'']$
λ ::= $\{id_{pp}\}$

id_{pp_d} dest physical port
dla_d dest data link addr
na_d dest network addr
pn_d dest port number
act action (*allow* or *deny*)

acc ::= $(n, g)[:(\omega_{aa}, n_{aa})][:adm]$
pp ::= $\langle id_{pp}, \{\langle dla, \{na\}, [w, [c], \{\omega\}] \rangle\} \rangle$
fr ::= $\langle id_{pp_s}, id_{pp_d}, dla_s, na_s, pn_s, dla_d, na_d, pn_d, pr, act \rangle$

id_{pp_s} source physical port
dla_s source data link addr
na_s source network addr
pn_s source port number
pr protocol (TCP, UDP, ...)
sw ::= $\langle sw\_name, ver \rangle$

Where **acc** represent an account where n and g are, respectively, a username and a group defined

for ω^*, **pp** is a physical port (i.e., network interface), **fr** is a filtering rule. **"f"** specifies both the prerequisites and the effects of the action π on the resources (software) involved or not. **phy_acc[c]** means that, in order to perform operation π on object ω, a user must be in the same room as ω and own credential c (if specified). Here we describe the formal model elements only briefly because our aim is not to provide all the technical details of the method but rather to show how the approach is used as a safety model for an industrial system. All the details of the implementation of this static method by formal methods have been described by the work of Manuel Cheminod et al. **(see [11])**. The figure **2** presents some principal concepts modeled by the formal method. On this figure, the

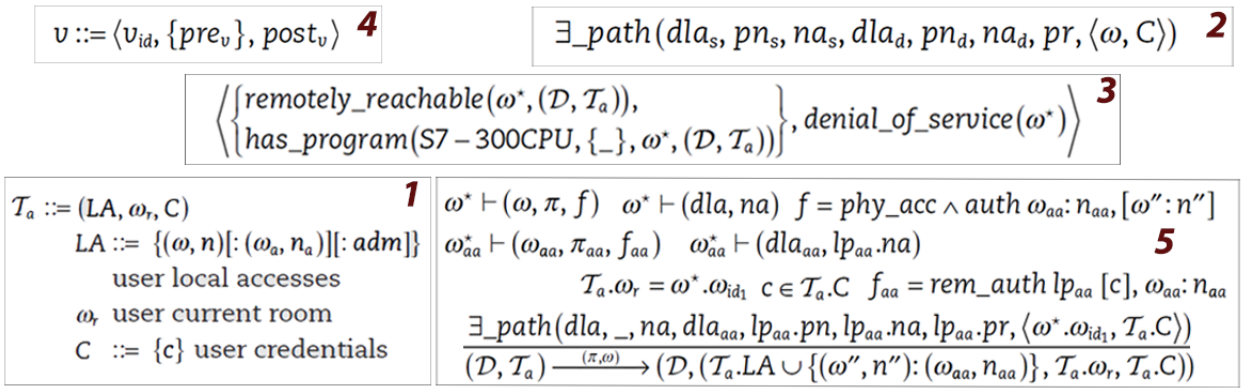

Figure 2: A partial description of the industrial system formal model

rectangle with the label (1) models the current state where the attacker is located, (2) models the wired or wireless path between two network components, (3) models the known vulnerability of the S7-300CPU software (possibility to remotely perform a bad action on the software causing a denial of service), (4) allows to model the concept of known vulnerability, and (5) represents an inference rule necessary to describe remote authentication mechanisms. The prototype implemented via Prolog using the formal model defined by this method, allowed to create a software tool which can be used by the security experts to design secure industrial networks.

5 Conclusion and perspectives

Ultimately, the risk analysis methods and safety models presented in this document are frequently used in the field of risk prevention, providing a systematic character of the analysis, making it possible to identify the causes and potential consequences of events related to the operation of industrial installations and highlight existing or potential risk barriers. After presenting the state of the art of risk analysis and prevention methods in industrial networks, the security models and the various challenges of industrial networks of the future taking into account the relationship with cyber security, we showed the importance of using the innovative approach "TVA" to construct attack graphs; which is an approach that takes into account both software vulnerabilities, network connectivity, behavior of firewall-type equipment, and exploits of potential attackers.

Finally, in the last section, after showing how to insert a security model in a global context of risk analysis in industry, we presented several existing security models including attack graphs, petri nets, formal methods, Bayesian and Monte Carlo approaches. This work allowed us to have a global view of the universe of analysis and risk prevention. This also allows us to say that there

is no good or bad method of risk analysis because each has advantages and disadvantages of its own; a particular method is therefore more or less adapted to the risk context of the system under study and the desired objectives to achieve. Further work will focus on research relating to more safety models in order to build models of which can totally adapt to the context of the industrial networks of the future.

References

[1] *Diagnostic des défaillances – Théorie et pratique pour les systèmes industriels*. Paris : Hermes, 1995.

[2] *Applied Security Visualization*. Addison Wesley, 2008.

[3] Leroy A. and Signoret J.P. *Le risque technologique (Que sais-je ?)*, page 124. Editions Presses universitaires de France, Paris, 1992.

[4] Villemeur A. *Sûreté de fonctionnement des systèmes industriels*, page 798. Paris : Eyrolles, Paris, 1988.

[5] ANSSI. Use case of cybersecurity for industrial control systems. Technical report, 2014.

[6] B. BEBRAY, S. CHAUMETTE, S. DESCOURIERE, and V. TROMMETER. Méthodes d'analyse des risques générées par une installation industrielle. Technical report, INERIS, DRA, 2006.

[7] Claude Berge. Theorie des graphes et ses applications. In *Collection Universitaire de Mathematiques*. 1958.

[8] Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon, and Riccardo Pucella. *TulaFale: A Security Tool for Web Services*, pages 197–222. Springer Berlin Heidelberg, 2004.

[9] Manuel Cheminod, Ivan Cibrario Bertolotti, Luca Durante, Paolo Maggi, Davide Pozza, Riccardo Sisto, and Adriano Valenzano. Detecting chains of vulnerabilities in industrial networks. *IEEE Transactions on Industrial Informatics*, 2009.

[10] Manuel Cheminod, Ivan Cibrario Bertolotti, Luca Durante, and Adriano Valenzano. Automatic analysis of security policies in industrial networks. *IEEE International Workshop on Factory Communication Systems*, 2010.

[11] Manuel Cheminod, Luca Durante, Lucia Seno, and Adriano Valenzano. Detection of attacks based on known vulnerabilities in industrial networked systems. *Journal of Information Security and Applications*, 2016.

[12] Manuel Cheminod, Luca Durante, and Adriano Valenzano. System configuration check against security policies in industrial networks. *Industrial Embedded Systems (SIES)*, 2012.

[13] The MITRE Corporation. Common attack pattern enumeration and classification, 2017.

[14] The MITRE Corporation. Common vulnerabilities and exposures, 2017.

[15] The MITRE Corporation. Nvd, national vulnerability database, 2017.

[16] The MITRE Corporation. Open vulnerability and assessment language, 2017.

[17] M.-C. Costa, D. de Werra, and C. Picouleau. Minimum d-blockers and d-transversals in graphs", j. of combinatorial optimization. *Journal of Combinatorial Optimization*, 2011.

[18] R. Dantu, K. Loper, and P. Kolan. Risk management using behavior based attack graphs. In *Conf. Information Technology: Coding and Computing*, 2004.

[19] J. Dawkins, C. Campbell, , and J. Hale. Modeling network attacks: Extending the attack tree paradigm. Technical report, Workshop Statistical Machine Learning Techniques in Computer Intrusion Detection, 2002.

[20] Information Technology Laboratory Department of Homeland Security's National Cyber Security Division, NIST Computer Security Division. National vulnerability database, 2017.
[21] Nikos Drakos and Ross Moore. Les différents types d'attaque, 2003.
[22] Sushil Jajodia and Steven Noel. Advanced cyber attack modeling, analysis, and visualization. Technical report, AIR FORCE RESEARCH LABORATORY, INFORMATION DIRECTORATE, ROME RESEARCH SITE, 2010.
[23] Sushil Jajodia and Steven Noel. Advanced cyber attack modeling analysis, and visualization. Technical report, George Mason University, 2010.
[24] K. Jensen, L.M. Kristensen, and L. Wells. Coloured petri nets and cpn tools for modelling and validation of concurrent systems. *International Journal on Software Tools for Technology Transfer*, 2007.
[25] Philippe Lagadec. Visualisation et analyse de risque dynamique pour la cyber-defense. In *Symposium sur la securite des technologies de l'information et des communications*, 2010.
[26] Zhi-Yong Liu and Hong Qiao. *Hidden Markov Model Based Intrusion Detection*, pages 169–170. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.
[27] Modarres M. *What every engineer should know about Reliability and Risk Analysis*, page 349. New York: Marcel Dekker, New York, 1993.
[28] Emmanuel MICONNET, Olivier BETTAN, Daniel GIDOIN, and Eric JOUENNE. Un exemple d'usage de graphes d'attaques pour l'evaluation dynamique des risques en cyber-securite. Technical report, Laboratoire d'Innovation ThereSIS, Thales Research and Technology, Campus Polytechnique, 2003.
[29] H. Niandou, A. Talon, D. Boissier, and L. Peyras. Analyse de risques : Identification et estimation : Demarches d'analyse de risques - methodes qualitatives d'analyse de risques, 2009.
[30] X. Ou. *A Logic-programming approach to network security analysis*. PhD thesis, Princeton University, 2005.
[31] Benjamin Picuira. Security database, 2017.
[32] Nayot Poolsappasit, Rinku Dewri, , and Indrajit Ray. Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 2012.
[33] Raffy. The davix live cd, 2008.
[34] I. Ray and N. Poolsappasit. Using attack trees to identify malicious attacks from authorized insiders. In *10th European Symp. Research in Computer Security (ESORICS '05)*.
[35] Kaplan S. *The words of Risk Analysis*, page 798. Paris : Eyrolles, Paris, 1997.
[36] V. Shandilya, C. B. Simmons, and S. Shiva. Use of attack graphs in security systems. *Journal of Computer Networks and Communications*, 2014.
[37] Oleg Sheyner and Jeannette Wing. *Tools for Generating and Analyzing Attack Graphs*, pages 344–371. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.
[38] Yuanzhuo Wang, Jingyuan Li, Kun Meng, Chuang Lin, and Xueqi Cheng. Modeling and security analysis of enterprise network using attack–defense stochastic game petri nets. *Security and Communication Networks*, 2013.