An Approach to Assess Risks Related to Information System in Supply Chain

Selmen Boubaker, Samuel Dumondelle, Parisa Dolatineghabadi

An Approach to Assess Risks related to Information System in Supply Chain

Selmen BOUBAKER[1], Samuel DUMONDELLE[1] and Parisa DOLATINEGHABADI[1]

[1] Capgemini Engineering, France
Selmen.boubaker@altran.com

Abstract: On one hand, no one can deny the importance of the information system in today's industrial and logistic activities. The progress in IT tools and systems allowed to process real-time data giving the opportunity to enhance considerably the management of production and transportation operations. On the other hand, supply chain digitalization is a sensitive process that can generate increased risks for the companies' activities. Therefore, such risks should be identified and managed. In this study, we follow Failure Mode, Effects, and Criticality Analysis (FMECA) approach to assess the risk linked to the information system of supply chains. We also present the methodology and choices adopted to apply this study in an aeronautical supply chain case.

Keywords: supply chain digitalisation, information reliability, information risk analysis, FEMCA

1 INTRODUCTION

Many industries have started their transition to the Industry of the Future (Industry 4.0) with the ambition of deploying a more agile, autonomous, environmentally responsible, and productive organisation. Big Data, Internet of Things (IoT) and artificial intelligence are taking place at all levels of the value chain to enable the automation of information and production flows. However, despite the considerable advances observed in recent years in the industry, the supply chain (SC) seems to lag behind the deployment of these technologies, which comes also with additional risks affecting its overall activities. Many authors highlighted the importance of virtualization and IT systems to enhance the values in supply chain activity. However, this will only be possible with the presence of reliable and secure information systems [1–4]. Indeed, if many IT risks have always existed in the economy, those related to SC are becoming more and more important with consequent impacts. We note the WannaCry cyber-attack on Renault, which in May 2017, which caused production interruption in several plants. "What is certain is that the IT networks of major manufacturers are now closely connected to those of their suppliers, to enable just-in-time stock management"[5]. This attack also affected around a hundred countries [6].

Current studies related to risks in SC are mainly conducted from logistics, economics, management or safety/health perspectives [7] . Although we find in the literature, the studies related to information flows and their risks, they are oriented towards IT flows and information systems, and therefore do not cover all information flows. Other studies are more specific to the Security of Information Systems in SC [8].

In this study, we focus on assessing the risks associated with information flows of SC in order to present preventive measures to enhance the information's flow reliability. An FMECA approach is used in order to identify and assess risks and then present preventive measures. A case from the aeronautical sector is studied relying on supply chain experts' experience and opinions.
This paper is organized as follows. In section 2, we present the literature review on risk analysis methods in SC and other industry sectors. In section 2, we describe the adopted FMECA methodology for this study. In section 3, we scrutinize different steps followed and results obtained. Finally, we present conclusion and perspectives for further researches.

2 Literature review

Nowadays, industries are moving toward modern's network connections thanks to the new technological infrastructures. Supply chain is not excluded from this trend. These changes require new secure and mobile services. Therefore, it is necessary to move to connected IP systems, which are secure, reliable and efficient [9].One way to make a system reliable and efficient is to identify well risk. In this section, first, we present the main concepts linked to the risk assessment and management. Second, we study risk analysis methods used in the literature and industry.

2.1 The concepts of reliability, safety and risk

In order to succeed in the transition toward supply chain 4.0, supply chain information systems must be reliable and secure. Reliability, according to the Cambridge dictionary, is "how accurate or able to be trusted someone or something is considered to be»[10]. According to ISO, it is the "Ability of an entity to perform a required function, under given conditions, during a given time interval"[11]. The concept of safety is more diverse. Safety according to [12] is " the probability, that no catastrophic accidents will occur during system operation, over a specified period of time". These two concepts, Reliability and Safety, together with Availability and Maintainability are the four key concepts of Dependability. "Dependability is the science of failures. It covers the concepts of reliability, availability, maintainability. and safety" [13].However, in order to control dependability, we need to assess and control risks. Risk is defined as the danger, or the possibility of danger, defeat, or loss. According to ISO, a risk is "a combination of the probability of a damage and its gravity" [11].

2.2 Risk analysis methods

There are several commonly used risk analysis methods. In the study presented in [14], we find a comprehensive classification approach to determine their choice of use.
We chose the FMECA, a method that allows both, to anticipate risks, and, to capitalize on feedbacks. It permits to identify all potential failures and failure modes, evaluate risks and prioritize actions to be taken. Moreover, FMECA is the most widespread method in the industry, and the most versatile [15].

It should be noted that numerous methods and tools have been developed for analyzing information system risks. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE method used in [16] allows to define a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. However, OCTAVE is complex to deploy, considering that the main users for this method could be from small companies with limited resources. The French Information Security Club developed the Harmonized Method of Risk Analysis method (MEHARI). "MEHARI's general approach consists in analyzing security issues: what are the feared scenarios? and in the prior classification of IS entities according to three basic security criteria (confidentiality, integrity, availability). These issues express the dysfunctions that have a direct impact on the company's activity. Then, audits identify the vulnerabilities of the IS. And finally, the actual risk analysis is done.". [17] uses The Threat Assessment & Remediation Analysis (TARA). The greatest strength of TARA also represents its greatest weakness. It only focuses on the greatest risk and less impacting risks are ignored. [18] presents the OWASP Software Assurance Maturity Model. OWASP only focuses on some subsets of threats in very specific environment. These methods must be managed by dedicated structures such as IT departments.

Although FMECA is widely used for process flows, few works in the literature are relating to information flows [19]. The information flow is present in these works as a component of which we give relatively little importance, the analysis focuses only on material flows. In our study, we focus on analyzing risks linked to the information flow using an FMECA analysis presented in the following section. This choice is also taken up in [20] for their study on the reliability of data in a management information system. FMECA approach is a tool that allows detecting the possible critical points and propose improvements. This approach has been used in different sectors including Supply Chain. The application of this approach in farming and food supply chain has resulted in proposing improvements in the traceability system focusing on the most severe situations from a systems criticality point of view [21].

3 Methodology: FMECA analysis

An FMECA analysis is carried out in a multidisciplinary participatory mode. The method takes place in five major stages. We adopt the same definitions of elements presented in [22]:

1. Preparation where we define the working group, the scope of the analysis, and the procedure to be followed.
2. Functional analysis, which aims to list all the phases of the process in order to identify the potential causes of malfunctioning and to prepare the study of failures.
3. Failure identification and rational study of failure modes.
4. Failure evaluation and criticality study and failure hierarchy.
5. Actions to be identified to search for solutions.

   In the following paragraphs, we present details of these steps and choices taken for our study.

3.1 Preparation: To define the working group, the scope of the study

Working group: an expert of quality management with significant experience in managing the deployment of FMEA in the industry was chosen as a moderator to guarantee the method, manage and ensure the follow-up of the analysis. A multidisciplinary working group of seven members was selected for their skills and their significant experience in SC, particularly in aeronautics sector. These participants have professional experiences from five to twenty years, acquired in the industry, and mainly within aeronautical industrials such as AIRBUS, STELIA, and SPIRIT. Their functions in the procurement, planning or logistics departments have enabled them to use and master information tools as well as business procedures. During their experiences, the participants were able to observe, as actors or observers, various malfunctions of all kinds and with various consequences, observed at various levels of SC. The working group had prior awareness of the FMECA method.
The scope studied: flows of information in an aeronautical supply chain is defined as the scope of this study. We study all IT tools used such as enterprise resource planning (ERP) and other information flows such as e-mails, EDI, and customer/supplier portals. Manuscripts, as physical information sources, are still widely used in industry. Only some flows were not taken into consideration, such as e-mails and faxes. Phone communications were considered as a secondary, informal means of communication rather than a formal information flow. Moreover, as these flows are not limited to the analyzed entity, but also to its environment, including suppliers and customers, the study covers internal and external information flows. This study cannot cover entirely all companies, because "FMECA is based on an inductive search for causes" [20]. This implies the use of factual data with evaluations of criteria to be individualized for each company. The aim of this analysis is to present a base for studies, not only for aeronautical companies and aeronautical suppliers, but also for all other manufacturing industries.

During this preparation stage, we chose tools to be used for our study. We adopt the standard model of the risk matrix presented in [23]. However, for this study, columns that are not relevant to the monitoring of actions were not used: the pilot of the action, the dated objective, the validation of the action, etc. Other columns were added in order to facilitate data filtering .For the criteria grids and ratings, there are no imposed models. However, some proposed models can be found in the literature. A scale of 1 to 4 with 4 criteria for a hospital supply chain was used in [19]. A scale of one to five with five criteria for a study on management information systems in the textile industry was chosen in [24]. [20] used a more complex grid with a scale of one to ten with ten criteria, close to the FMEA 4th Edition at Caterpillar [25]. We choose a scale of one to ten to rate severity, frequency and detectability on a scale of one to ten, choosing only four criteria: one, three, six and ten to have a significant difference in criticality.

3.2 Functional Analysis: Preparing a functional breakdown and preparing the failure study

A group of consultants with significant experiences in the aeronautical supply chain carried out mapping (see Fig. 1), starting with a representation of the macro and semi-macro physical flows. Maps are completed later by adding the information flow.

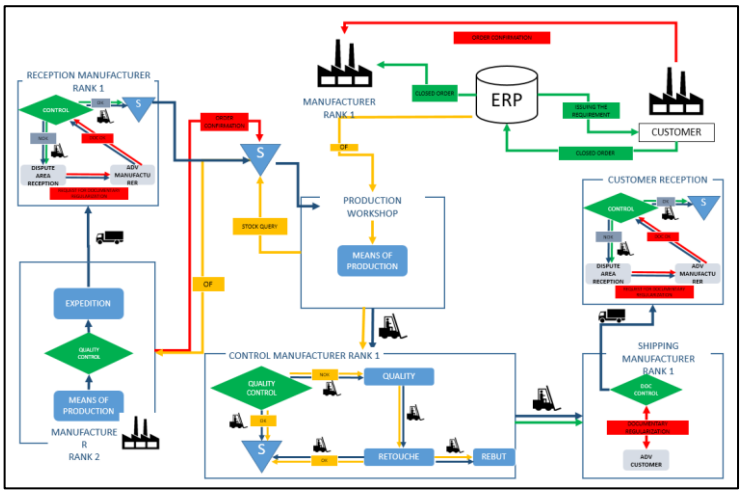


Fig. 1. Extract from the upstream flow map

Based on the items and information flows identified in the maps, we have broken down this process into activities in a Value Stream Mapping (VSM). Each activity is detailed: who is responsible for it, what is the nature and medium of the information exchanged. These VSMs obtained will be served as a basis for building the FMECA in the next step.

3.3 Preparation of the FMECA grid

We integrated each line of the VSM obtained previously into the FMECA grid, then after analyzing the nature of each flow and each action, only lines corresponding to the information flow were kept.
We note that some line groupings have been created. Indeed, some tasks/actions are repeated throughout the SC. Grouping these tasks results in a more visible table, but above all, when modifying or updating the information added, we have to ensure that the information is consistent at all stages. Five groupings, called Blocks, were created: Block Co for control, Block Re for Reception, Block SP for Production Monitoring and Block Tra for Transfer (between workshops or stations).

3.4 Identification: identify failures and make a rational study of failure modes

Ishikawa analysis

To begin the analysis, we have determined, based on consultants' experience, what could be the most impactful and frequent problem along with the SC information flow. By its nature, ERP (including SAP) is the system that we find throughout the SC in industry, with external links with suppliers and customers. We have excluded the telephone, e-mail, and fax. In fact, they are only used to support the use of the ERP and generally in an informal way.

The problem identified is "The information transmitted by the ERP is deficient (No information, Incomplete information, Incorrect information etc....)".
We use the Ishikawa method to determine the different possible causes of the problem. During a brainstorming session, the working group listed the different potential failures that can disrupt the information flow of an ERP in a global way. So starting from the effect, we identify the possible causes of this problem, then define the causal chain by the five whys method. For each effect, we studied the possible direct causes. For each direct cause, we examine the possible secondary causes. The process consists of asking questions up to five times in order to determine the root cause.
The next step is discernment, where only relevant causes are kept. These causes are classified into five families of possible causes: Materials, Machines, Methods, Manpower, and Environment [26]. We have added Management as possible sources of a problem. In our study, we have determined that information is the primary material. Therefore, all causes related to the information transmission are in the category of the first subject. For the hardware, we take all the causes related to computers (computers and software), and networks (computer and electrical or computer, electrical, etc.). Using this analysis, we find all causes linked to the settings and operator modes linked to the workforce failures. For those linked to the environment, we find causes linked to the work environment as well as external disturbances. For the management, we identify mostly causes linked to hierarchical decision-making.

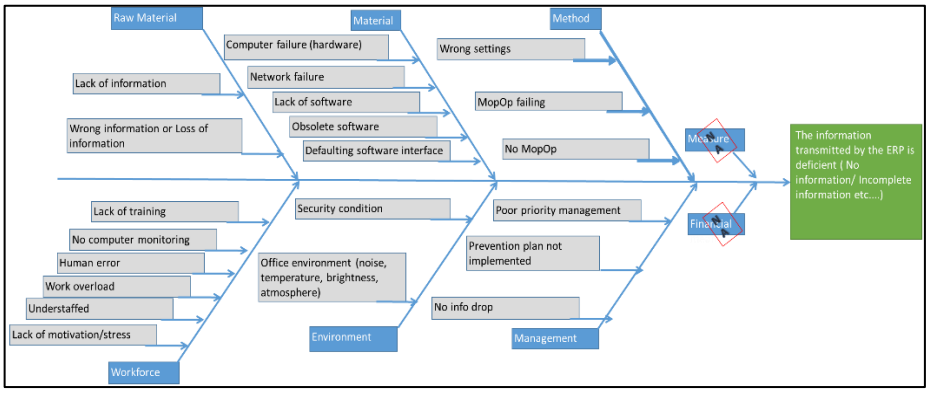


Fig. 2. Ishikawa analysis for the information flow of the supply chain

Identification of failure modes.
There are five categories of generic failure modes [22]: 1) Loss of function, 2) Untimely operation, 3) Unable to start, 4) Unable to stop, 5) Degraded operation.
In our study, we identify three failure modes: loss of function, inconvenient operation and degraded operation. In precise technical terms, for loss of function: Information not transmitted, information not processed, operation not carried out. For degraded operation: incomplete information, poor transcription of information, poorly performed operation.
In the FMECA grid, for each existing line, taken from the VSMs, we must analyze all the potential failure modes. For this research, we use the generic modes, the precise terms but also the "generic" analysis carried out with the Ishikawa method on the ERP

information flow. For each line, the group asks the question: How can this not work? For example, if the function is “calculation of the part requirement”, the responses were “calculation of the requirement does not work (Loss of function)” and “calculation of the requirement does not work properly, we are obliged to launch a command manually (Degraded operation)”.

Search for causes of failure

For each failure mode, for each line of the VSM concerned by an information flow, we define the potential causes. We use data and causes already determined by the Ishikawa of the generic ERP information flow when this risk analysis is transposable. The experience of each member of the working group allows us to identify/recognize potential causes (Table 1).

Study of the effects

In this step, we look for the effect that has the greatest impact on the company. Shorted by its importance, we look for the effect on the customer/human safety (physical risk, environmental risk). Then, we investigate the effect on customers (delay in delivery). Then, we distinguish the major effect on the company or the process (line stoppage, stoppage with disruption of production), the minor effect on the company or the process (stoppage without disruption of the line), and the case of no significant effect. We note that for the lines resulting from the Ishikawa analysis, the causes indicated are the root causes. For the other lines, the causes noted are the primary causes (Table 1).

Table 1. Extract from the FMECA table

Process activities	Process sub-activities	Failure modes	Causes	Effects	Means of detection
Release of parts requirements	calculation of net requirement (MRP)	degraded operation (manual control)	Parameter error	order delay	auto control
Release of parts requirements	calculation of net requirement (MRP)	Information not transmitted	Computer problem	No command	auto control
Release of parts requirements	calculation of net requirement (MRP)	loss of function	Parameter error	No command	SAP transaction or excel export
Release of parts requirements	calculation of net requirement (MRP)	loss of function	Computer problem	No command	minimum stock alert for VMI

Survey of existing detection means

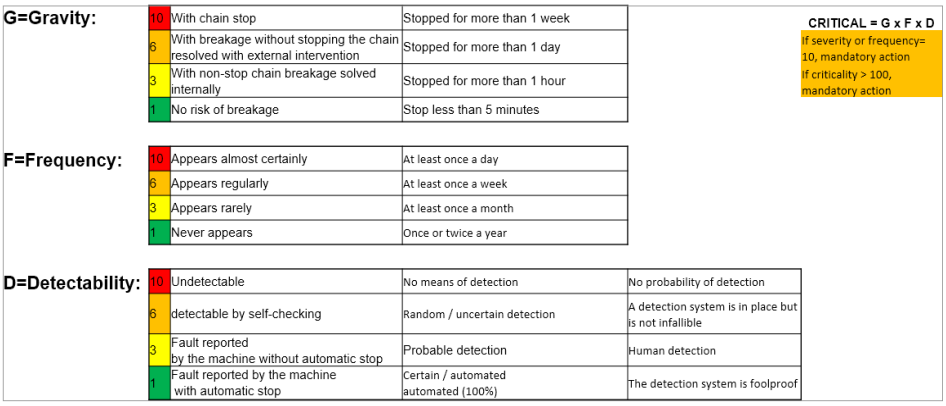
For each failure mode, we search for existing detection means, which are of a technological nature (ERP alert, printer alert, etc.) or human (self-checking, visual control).

Evaluating identified failures and studying their criticality

It is now a question of quantifying the risks. To do this, the FMECA method defines quantification criteria to which a score will be assigned.

- The frequency of occurrence (F): it indicates how often cause of the failure will occur.
- The gravity (G) or severity (S): that is the evaluation of the importance of the effects of the failure on people and/or the installation.
- The risk of non-detection (ND), often paradoxically called detection (D): the probability that the cause and the mode has occurred and the failure will reach the user.

Fig. 3 presents the rating criteria grids adopted corresponding to (G), (F) and (D)



G=Gravity:			
	10	With chain stop	Stopped for more than 1 week
	6	With breakage without stopping the chain resolved with external intervention	Stopped for more than 1 day
	3	With non-stop chain breakage solved internally	Stopped for more than 1 hour
	1	No risk of breakage	Stop less than 5 minutes

CRITICAL = G x F x D

If severity or frequency= 10, mandatory action

If criticality > 100, mandatory action

F=Frequency:			
	10	Appears almost certainly	At least once a day
	6	Appears regularly	At least once a week
	3	Appears rarely	At least once a month
	1	Never appears	Once or twice a year

D=Detectability:				
	10	Undetectable	No means of detection	No probability of detection
	6	detectable by self-checking	Random / uncertain detection	A detection system is in place but is not infallible
	3	Fault reported by the machine without automatic stop	Probable detection	Human detection
	1	Fault reported by the machine with automatic stop	Certain / automated automated (100%)	The detection system is foolproof

Fig. 3. Rating criteria grids

3.5 Corrective actions: Identification of preventive actions, palliative/curative actions, corrective actions

For each failure, actions are proposed to reduce criticality. These actions may relate to severity, frequency or detectability. Thus, for an action that acts on the cause of a failure, we expect an improvement in the frequency of this failure after the action has been implemented. A better means of detection should decrease detectability.
We can note that gravity is a little bit improved by actions. Indeed, generally, the actions that improve gravity are either design-related (in the case of a product) or require significant investments. In our study, it is the multiplication of networks and back-up systems. We can consider that an effective action must improve the factor by one level. Thus, it takes two detective actions to decrease the detectability from ten to three (with our evaluation grid).For each action, a new valuation must be carried out taking into account the expected effects of these actions. The objective is to reduce these criticalities below the defined threshold, 100 in our study.

4 Conclusions and perspectives

No one can deny the importance of the information system for supply chain activities. Therefore, it is essential to assess and manage increasing risks linked to information flows in the supply chain. In this paper, we present a FMECA approach allowing the assessment of risks associated with the information system of supply chains. As a result,

368 risks were identified. Thirty risks have a criticality of 360 (gravity *detectability*frequency), 145 have a criticality more than 180 and 221 have a criticality more than 100. Concerning causes of failures, 181 are related to the working force and 109 to materials (computer networks and software). Out of 368 proposals to mitigate risks, 149 are related to staff training/awareness and 81 are hardware-related, of which 45 can be addressed by an Information Security Management System (ISMS). However, 130 (out of 149) proposals related to training / awareness could be transformed into technological actions (IOT or AI).As a conclusion, it is noticeable that human error is still one of the major risks associated with the flow of information in SC. Despite the work that companies are doing to raise awareness among their employees, these actions are still limited and the solution can be to automate more data entry activities and to integrate more advanced data entry control systems.
This work can be a basis for further researches aiming to evaluate and enhance the supply chain information system's reliability.

References

1. Dobrovnik M, Herold DM, Fürst E, Kummer S (2018) Blockchain for and in Logistics: What to Adopt and Where to Start. Logistics 2:18. https://doi.org/10.3390/logistics2030018
2. Francisco K, Swanson D (2018) The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. Logistics 2:2. https://doi.org/10.3390/logistics2010002
3. Prause G (2019) Smart Contracts for Smart Supply Chains. IFAC-PapersOnLine 52:2501–2506. https://doi.org/10.1016/j.ifacol.2019.11.582
4. Banerjee A (2018) Chapter Three - Blockchain Technology: Supply Chain Insights from ERP. In: Raj P, Deka GC (eds) Advances in Computers. Elsevier, pp 69–98
5. (2017) Renault, un mois et demi après WannaCry. In: Les Echos. https://www.lesechos.fr/2017/06/renault-un-mois-et-demi-apres-wannacry-156961. Accessed 4 Feb 2021
6. (2017) Cyberattaque mondiale : Renault-Nissan dans l'œil du cyclone. Le Monde.fr
7. Tapiero CS (2008) Analyse des risques et prise de décision dans la chaîne d'approvisionnement. Revue francaise de gestion n° 186:163–182
8. Ruel S, Ouabouch L (2015) Paradoxe du système d'information dans la supply chain : vecteur de performance ou facteur de risques ?
9. Boiko A, Shendryk V, Boiko O (2019) Information systems for supply chain management: uncertainties, risks and cyber security. Procedia Computer Science 149:65–70. https://doi.org/10.1016/j.procs.2019.01.108
10. Cambridge Dictionary | English Dictionary, Translations & Thesaurus. https://dictionary.cambridge.org/. Accessed 17 Mar 2021
11. ISO.Org (1999) ISO/CEI Guide 51:1999(fr). https://www.iso.org/obp/ui/#iso:std:iso-iec:guide:51:ed-2:v1:fr. Accessed 14 Feb 2021
12. Mulazzani M (1985) Reliability versus safety. IFAC Proceedings Volumes 18:141–146
13. Avizienis A, Laprie J, Randell B (2001) Fundamental Concepts of Dependability
14. Mazouni MH (2009) Pour une meilleure approche du management des risques: de la modélisation ontologique du processus accidentel au système interactif d'aide à la décision. 239

15. Thoppil NM, Vasu V, Rao CSP (2019) Failure Mode Identification and Prioritization Using FMECA: A Study on Computer Numerical Control Lathe for Predictive Maintenance. J Fail Anal and Preven 19:1153–1157. https://doi.org/10.1007/s11668-019-00717-8
16. Caralli R, Stevens JF, Young LR, Wilson WR (2007) Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. 951038 Bytes. https://doi.org/10.1184/R1/6574790.V1
17. Wynn, Jackson Whitmore, Joseph Upton, Geoff Spriggs, Lindsay McKinnon, Dan McInnes, Richard Graubart, Richard Clausen, Lauren (2011) Threat Assessment & Remediation Analysis (TARA): Methodology Description Version 1.0
18. Chandra P (2008) Software assurance maturity model. A guide to building security into software development v1 0, OWASP Project
19. Kahla -Touil IB (2011) Gestion des risques et aide à la décision dans la chaîne logistique hospitalière : cas des blocs opératoires du CHU Sahloul. Phdthesis, Ecole Centrale de Lille ; Institut Supérieur de Gestion de Sousse
20. Bironneau L, Martin D, Parisse G (2010) (PDF) Fiabiliser les données d'un système d'information de gestion par la méthode AMDEC : principes et études de cas. In: ResearchGate. https://www.researchgate.net/publication/282059106_Fiabiliser_les_donnees_d'un_systeme_d'information_de_gestion_par_la_methode_AMDEC_principes_et_etudes_de_cas. Accessed 29 Jan 2021
21. Bertolini M, Bevilacqua M, Massini R (2006) FMECA approach to product traceability in the food industry. Food Control 17:137–145. https://doi.org/10.1016/j.foodcont.2004.09.013
22. Rapinel J-B, Sebti H Préparation de l'AMDEC - Groupe de travail - Compétence. http://amdec.fmeca.free.fr/preparationAMDEC31.html. Accessed 29 Jan 2021
23. AIAG A (FMEA) Failure Mode & Effects Analysis | AIAG. https://www.aiag.org/quality/automotive-core-tools/fmea. Accessed 28 Jan 2021
24. Mansour S La place de l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité(AMDEC) dans l'industrie. 6
25. Shaffer C FMEA Quick Reference
26. Saizy-Callaert S, Causse R, Thébault A, Chouaïd C (2002) Failure Mode, Effects and Criticality Analysis (FMECA) as a means of improving the hospital drug prescribing process. International Journal of Risk & Safety in Medicine 15:193–202