Cyber risk and machine safety: towards the integration of cyber risk assessment into occupational risk assessment?

Lamy P., Perrin N., Ghadban N.
Institut national de recherche et de sécurité (INRS)
1 rue du Morvan - CS 60027
F-54519 VANDŒUVRE cedex
pascal.lamy@inrs.fr, nellie.perrin@inrs.fr, nisrine.ghadban@inrs.fr

KEYWORDS: cyber risk assessment, connected machines, cybersecurity, machine

ABSTRACT

In the rapidly evolving landscape of industrial technology, the integration of production systems and machinery is reaching unprecedented levels of interconnectedness. This interconnectedness, while promising efficiency gains, also raises significant concerns about the security of machine safety systems and the safety of workers. To address these challenges, INRS has launched a pioneering study focused on developing a specialized methodology for assessing cyber risks associated with machinery. Collaborating with occupational ergonomist and psychologist, the study entails a comprehensive survey to gauge the current state of machine connectivity and cybersecurity practices within companies. By gathering these informations, the survey aims to contribute to our subsequent work aimed at bolstering cybersecurity protocols and safeguarding industrial workers. On another side, this survey will help us to gather workers' perception of the risk of cyber-attack and its impact on their health and safety. Through this multidisciplinary approach, INRS aims to enhance our understanding of the intricate relationship between machine connectivity, cyber threats, and occupational safety, fostering more resilient and secure industrial environments.

1 CONTEXT

The Industry of the Future exposes machinery to heightened vulnerability to cyber attacks, attributable to the expanded attack surface in cybersecurity. With machinery components like sensors and actuators interconnected to the company's IT network, the accessibility to these systems is amplified, particularly with the use of connected components or sensors (IIoT). Consequently, this connectivity facilitates potential avenues for cyber attacks through digital vectors.

Traditionally, cyber attacks primarily resulted in data breaches or disruptions to IT systems, impacting the company's operations. However, there's been a discernible evolution in the nature and consequences of these attacks, extending to industrial and professional risks. For employees, diverse impacts are foreseeable in the event of a cyber attack:

- Property damage risk to installations or industrial processes, such as explosions or release of hazardous substances.
- Compromising safety functions on machinery, endangering employees by allowing hazardous machine movements.
- Misrepresentation of machine status, potentially leading employees into unsafe situations.
- System failures necessitating urgent maintenance interventions, elevating the risk of accidents due to time pressures.
- Psycho-social risks like stress, increased workload, and job security concerns stemming from data loss or theft, impacting the workforce's well-being and organizational dynamics.

With the evolving landscape in the Industry of the Future, particularly the digitization of data, the threat of cyber attacks on manufacturing systems is increasingly prominent [1] [2]. Machinery presents a prime target for such attacks, given the limited consideration of cyber risks by manufacturers and machinery designers alike.

Recent studies underscore the potential consequences of cyber attacks on industrial systems. For instance, a study [3] highlights how a cyber attack on a robotic installation could alter the robot's manual mode, endangering worker safety by increasing collision risks. Another study [4] reveals vulnerabilities in wireless industrial remote controls, which, if exploited, could pose risks to employees by enabling unauthorized control over machinery movements, potentially leading to accidents. Furthermore, a study on numerical control machines [5] mentions the possible effects on the security of the operator following the disabling of a feed hold function. This function can be requested by the operator to control the machining before launching the production.

Recognizing these risks, regulations governing machinery design in the European market, like Regulation 2023/1230 [6] of the European Parliament, have incorporated provisions to address cyber threats. This regulation repeals the Machinery Directive 2006/42/EC with effect on 14 January 2027. It introduces aspects on the protection against corruption and malicious (intentional) behaviour, which therefore must be considered in the future. In its Annex III, §1.1.9 specifies that "a hardware component transmitting signal or data, ... shall be designed so that it is adequately protected against accidental or intentional corruption". The same applies for "software and data that are critical for the compliance of the machinery or related product with the relevant essential health and safety requirements shall be identified as such and shall be adequately protected against accidental or intentional corruption". More specifically for control systems, 1.2.1a of this same annex III specifies that "control systems shall be designed and constructed in such a way that they can withstand, where appropriate to the circumstances and the risks, the intended operating stresses and intended and unintended external influences, including reasonably foreseeable malicious attempts from third parties leading to a hazardous situation".

However, for companies utilizing machinery, especially SMEs, awareness of cyber risks and expertise in mitigating them may be lacking [7]. Efforts are underway to integrate cyber risk considerations into safety assessments, aiming to bridge the gap between safety and security in industrial operations [8-10]. To address this gap and to see how to include cyber risk into occupational risk assessment, the INRS is spearheading a study to develop a cyber risk assessment approach tailored to machinery users. This approach aims to analyze the potential impact of cyber attacks and integrate cyber risk assessment into existing occupational safety protocols. By identifying threats, vulnerabilities, and potential attack scenarios, this approach will enable companies to better understand and determine the risks for the employee posed by cyber attacks on industrial machinery.

The rest of this paper is organized as follows: Next section describes the strategy for the study. In section 3, we describe how we collect information via questionnaires in order to build the cyber risk assessment. Section 4 gives the structure of questionnaires. Section 5 concludes the paper.

2 TOWARD A CYBER RISK ASSESSMENT FOR MACHINERY IN OCCUPATIONAL RISK ASSESSMENT?

In the first phase of the INRS study, we are developing the Cyber Risk Assessment for Machinery (CRAM) methodology. Drawing on the expertise of the INRS' Information Systems Security Manager and existing literature on cyber risk assessment, we are refining the CRAM methodology based on survey results (Figure 1).

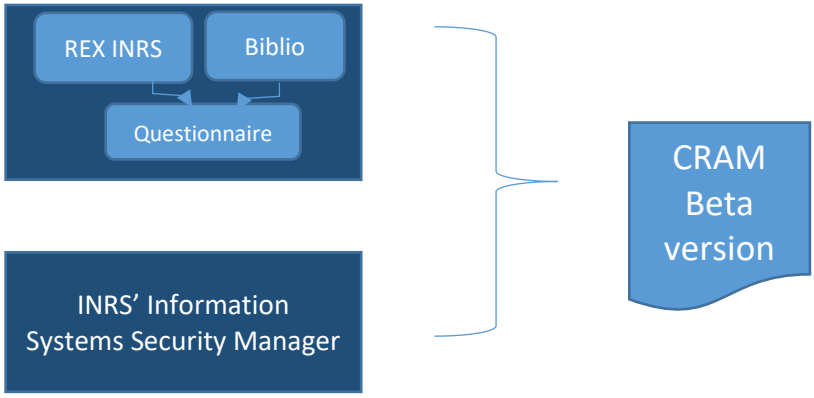

Figure 1. *Drawing up of the Cyber Risk Assessment for Machinery*

The second phase involves implementing this methodology on at least one of the INRS' machines to validate its practicality. This includes assessing clarity, comprehensibility of terms, absence of ambiguity, and overall clarity

and duration of the method. Any necessary improvements will be incorporated to finalize the 1.0 version of the cyber risk assessment for machinery (Figure 2).

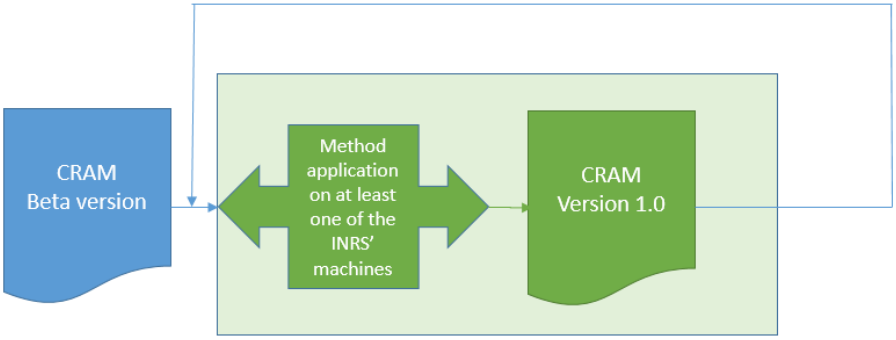

Figure 2. *Application and Evaluation of Cyber Risk Assessment for Machinery: Method Validation and Comparative Analysis*

Depending on the feasibility and applicability considerations, including the duration of analysis, we may extend the cyber risk assessment to multiple industrial machines available at the INRS (test beds available at INRS). Our priority is to internally assess the operational effectiveness of the methodology, which will involve collaboration with a dedicated workgroup comprising INRS staff familiar with the selected machine, professionals experienced in risk analysis, and the INRS' Information Systems Security Manager. This application phase will focus on analyzing the selected machine to identify cyber risks and their potential impacts. The insights and expertise gathered from the workgroup discussions will guide us in determining the practicality and suitability of the cyber risk assessment for machinery.

In the subsequent third phase, we will compare the outcomes of our methodology's implementation with those obtained from two established "complex" cyber risk assessment methods tailored for industrial systems. These methods include IEC 62443-3-2 [11] and EBIOS Risk Manager, adapted for industrial applications [12]. This comparative analysis aims to ensure the comprehensiveness of our cyber risk assessment approach for machinery and to assess its strengths and limitations effectively. Therefore, we aim to validate the methodology's effectiveness, refine its application, and provide insights into its comparative performance against established industry cyber risk assessment. This iterative process will contribute to the ongoing development and enhancement of cyber risk assessment practices tailored for industrial machinery.

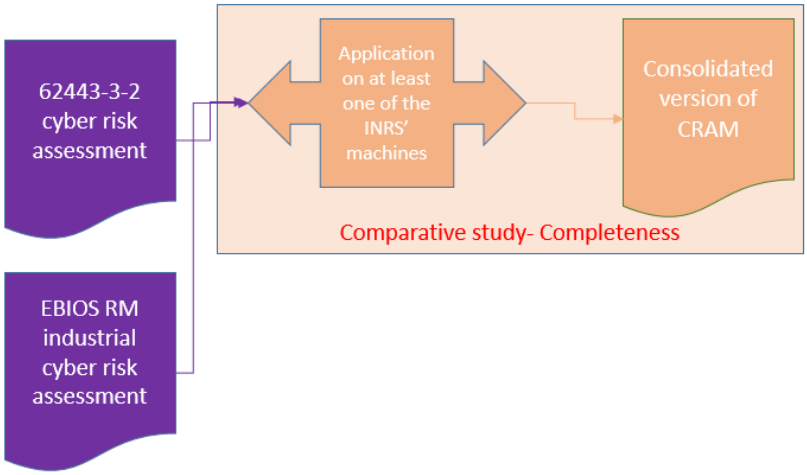

Figure 3. *Comparative study*

Note that we will apply the two additional cyber risk assessment methods to the same machine(s) considered in the preceding step. Through this process, we aim to compare the outcomes of the various methodologies: identifying common scenarios, noting any discrepancies, assessing the depth of analysis, and evaluating the time and complexity of implementation. By scrutinizing these parameters, we can determine the efficacy of each method and explore opportunities for enhancement. This comparative stage holds the potential to refine and improve the cyber risk assessment methodology for machinery.

In the fourth and final phase, we will examine the interplay between the cyber risk assessment for machinery and occupational risk assessment. Drawing on insights gained from applying the cyber risk assessment to INRS machinery, our objective is to establish a framework for integrating these assessments effectively. Specifically, we seek to understand how the cyber risk assessment can complement existing occupational risk assessments, whether through sequential or parallel analyses, or through a combination of approaches.

The cyber risk assessment for machinery will offer insights into potential impacts of cyber attacks, such as data corruption or software manipulation. Firstly, we will assess these impacts from an Occupational Health and Safety perspective, determining if they affect existing protection measures. For instance, if a cyber attack compromises software managing a safety function, resulting in its loss, we must ascertain if this impacts existing risk management protocols.

Furthermore, we will explore additional questions, including:

- Can cyber attack scenarios that affect functional aspects introduce new occupational risks?
- Can the implementation of cybersecurity measures inadvertently introduce new hazards? i.e. emergence of a new dangerous situation following the implementation of cyber protection measures.

Through practical examples and procedural guidance, we aim to demystify the integration of cyber risk considerations into occupational risk assessments, providing valuable insights and assistance to companies seeking to enhance their occupational risk management practices.

3 HOW TO COLLECT INFORMATION IN ORDER TO BUILD THE CYBER RISK ASSESSMENT?

Conducting a comprehensive cyber risk assessment entails mapping out potential malicious attack scenarios, which hinge on exploiting vulnerabilities and understanding access points to equipment and materials. To construct actionable scenarios for cyber risk assessment, it is crucial to grasp the attack surface — how machinery is utilized, accessed (e.g., via USB keys, remote programming, or maintenance), and connected.

To gather insights into these aspects, we have developed three questionnaires tailored to different stakeholders: one for production and EHS staff, another for maintenance personnel and innovation offices, and a third for IT personnel. Our aim is twofold: to identify weaknesses and entry points in machinery and leverage this information to propose fundamental actions for constructing attack scenarios, thereby facilitating cyber risk assessment for machinery. While detailed findings from these questionnaires are pending, several hypotheses merit exploration:

- Company size may influence awareness and mitigation efforts concerning cyber risks.
- Connected machinery with remote access points may pose heightened security risks.
- Worker safety might not be perceived as vulnerable to cyber attacks.
- Cyber attacks may be perceived as rare occurrences.
- Password policies within companies may require improvement.
- Internal resources dedicated to combating cyber risks might be lacking.

The questionnaires were developed in collaboration with occupational ergonomist-psychologist and administered electronically using Sphinx iQ3 software to ensure efficient distribution and maintain respondent anonymity and confidentiality.

4 STRUCTURE OF THE QUESTIONNAIRES

Each questionnaire comprises a core set of questions and sections tailored to specific audiences. These sections aim to gather insights on various aspects, such as individuals' perceptions of potential cyber attacks and their experiences as victims. Refer to Table 1 for a detailed breakdown of the questionnaire sections based on the three target groups.

Table 1. *The different sections of the questionnaires.*

Production-EHS target audience	**Maintenance-New works target audience**	**IT target audience**

General information	General information	General information
Connectivity and accessibility	Connectivity	Connectivity
	Accessibility	Accessibility
	Equipment, software and safety	
Cybersecurity	Cybersecurity	IT and cybersecurity
Consequences of a cyber attack	Consequences of a cyber attack	Consequences of a cyber attack

To ensure clarity and relevance, questionnaires comprise distinct sections designed to capture essential insights:

- General Information: This section is common to all the questionnaires and establish the company and respondent profiles, including sector, company size, position, seniority, age, and types of machinery used..
- Connectivity and Accessibility: This section provides a situational analysis of machine connectivity and access points. It explores aspects such as connection to company or industrial networks, use of data exchange mediums like flash drives, tablets, or smartphones, and management of remote and physical access.
- Equipment, Software, and Safety: Here, practices related to industrial programming and management of protective equipment (employee safety) are examined. It investigates how equipment is programmed or configured and the accessibility of safety features.
- Cybersecurity: This section assesses respondents' knowledge of cybersecurity, including awareness of risks, frequency of software updates, password policies, and existence of cyber risk assessments.
- Consequences of a Cyber Attack: This segment is common to all the questionnaires and evaluates the impacts of cyber attacks on company functioning and occupational health and safety. It also captures employees' perceptions and experiences in the event of a cyber attack.

5 CONCLUSION

In light of the growing connectivity of machinery and the widespread digitization of data facilitating various forms of data exchange, machinery is increasingly vulnerable to cyber attacks. These attacks pose not only the risk of disrupting production and incurring financial losses but also endanger the safety of workers. In our efforts to develop a comprehensive risk assessment methodology for cyber attacks on machinery, we conducted a survey using a structured questionnaire. This survey serves to elucidate the digital access points to machinery and aids in the formulation of attack scenarios, a critical step in the cyber risk assessment process.
We envision our work as a significant contribution to the integration of cyber risk considerations into occupational risk assessments. By shedding light on the specific digital vulnerabilities of machinery and identifying potential attack scenarios, we aim to enhance the safety protocols and risk management practices employed in industrial settings. Through this endeavour, we seek to foster a more holistic approach to risk assessment that encompasses both traditional occupational hazards and emerging cyber threats, ultimately safeguarding the well-being of workers and the integrity of industrial operations.

6 REFERENCES

1. Héry M., Malenfer M. - *Evolution des modes de production et risques professionnels : un état des lieux de la veille en 2017*. HST, 2018, 251, pp. 108-115.

2. Lamy P. – *Cyber attack: what are the impacts for occupational health and safety and more specifically for machine safety?* SIAS 2021, 10th International Conference of the Safety of Industrial Automated Systems, Japan.

3. Maggi F., Quarta D., Pogliani M., Polino M., Zanchettin A.M., Zanero S. - *Rogue Robots: Testing the Limits of an Industrial Robot's Security*. 2017, 48 p. https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf

4. Anderson J., Balduzzi M., Hilt S., Lin P., Maggi F., Urano A. *A security analysis of radio remote controllers for industrial applications*. Trend Micro

5. Balduzzi, M., Sortino, F., Castello, F., Pierguidi, L. (2023). *A Security Analysis of CNC Machines in Industry 4.0*. In: Gruss, D., Maggi, F., Fischer, M., Carminati, M. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2023. Lecture Notes in Computer Science, vol 13959. Springer, Cham. https://doi.org/10.1007/978-3-031-35504-2_7

6. Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (Text with EEA relevance), *OJ L 165, 29.6.2023, p. 1–102*

7. *Cybersécurité – Passons à l'échelle*. Rapport de l'Institut Montaigne, juin 2023, 158 p. Cybersécurité : passons à l'échelle | Institut Montaigne.

8. Dobaj J, Schmittner C, Krisper M, Macher G. *Towards Integrated Quantitative Security and Safety Risk Assessment.* In: Romanovsky A, Troubitsyna E, Gashi I, Schoitsch E, Bitsch F, editors. Computer Safety, Reliability, and Security, Cham: Springer International Publishing; 2019, p. 102– 16.

9. Kriaa S, Pietre-Cambacedes L, Bouissou M, Halgand Y. *A survey of approaches combining safety and security for industrial control systems.* Reliability Engineering & System Safety 2015;139:156– 78. https://doi.org/https://doi.org/10.1016/j.ress.2015.02.008.

10. Cormier A, Ng C. *Integrating cybersecurity in hazard and risk analyses.* Journal of Loss Prevention in the Process Industries 2020;64:104044. https://doi.org/10.1016/j.jlp.2020.104044.

11. AFNOR, NF EN IEC 62443-3-2 – *Security for industrial automation and control systems – Part3-2 : security risk assessment for system design*. AFNOR, août 2020, 31 p

12. Jean-Marie Flaus, Jean Caire. *EBIOS pour les systèmes industriels.* Congrès Lambda Mu 23 « Innovations et maîtrise des risques pour un avenir durable » - 23e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Institut pour la Maîtrise des Risques, Oct 2022, Paris Saclay, France. ⟨hal-03966629⟩