Toward a framework dedicated to the anticipation of consequences of a new technological system on safety performance.

Eric Rigaud, Thomas Côte

Toward a framework dedicated to the anticipation of consequences of a new technological system on safety performance.

Eric RIGAUD, Thomas COTE

Mines-Paristech, CRC – Centre de recherche sur les Risques et les Crises, BP 207 1 rue Claude Daunesse
06904 Sophia Antipolis Cedex

eric.rigaud@mines-paristech.fr, thomas.cote@mines-paristech.fr

Résumé – Cet article présente les premiers résultats d'un travail de recherche visant à la mise en œuvre d'un cadre méthodologique d'aide à l'identification des conséquences de l'introduction d'un nouveau système technologique au sein d'un système sociotechnique. L'article est structuré en deux parties. La première partie pose les fondements de la recherche à partir de considérations générales sur les conséquences d'un changement au sein d'un système complexe. La deuxième partie présente les objectifs et la structure générale du cadre méthodologique.

Abstract – This article is dedicated to the presentation of first results of a research activity related to the definition and the development of a framework dedicated to the assessment of consequences of the introduction of a new technological system in a socio-technological system. The article is structured in two parts. The first one is related to the presentation of the basement of the research with some generic consideration about consequences of change in complex systems. The second one is related to the presentation of the finality and s-the structure of the framework.

1. Introduction

The introduction of a new technological system in an organisation is the result of a strategic decision aiming to support the adaptation of the behaviour of the organisation to its environment. New technological system allowing increasing one or several performance dimensions such as cost effectiveness, flexibility, quality, security or safety.

The realisation of the technological change is generally completed by a risk analysis process aiming to identify hazards associated to the new system and by a change management process aiming to facilitate the adoption and the utilisation of the new system.

Despite those precautions, several examples can be found of occurrence of negative and perverse effects affecting negatively the performance of the organisation. Those negative effects can be related to the non-compatibility, to the inefficiency of the new system, to its rejection by the operators, to the creation of new dependencies or to the loose of flexibility and of margins of manoeuvre to perform tasks.

Those negative effects can have impacts on the financial performance of the organisation but can also be at the origin of incidents and accidents.

Technology assessment [1] aims considering the potential consequences of new technological system. Several methods and tools exist to support such assessment. In the context of safety and security, traditional risk assessment methods such as FMECA or THERP are often used with the purpose to identify potential risks related to the adoption of a new technology.

Such approaches allow considering a set of consequences but present some limitations regarding, among others things, to consider the complexity of human behaviours, of socio-technical systems and of large-scale socio-technical systems.

Objective of this paper is to present theoretical issues about anticipating the consequences of a change on the safety performance of a system, to present a first prototype of change management framework.

2. Theoretical issues about technological assessment

This section is about the presentation of a set of theoretical issues related to technological assessment. Three topics are addressed: technological system change diversity, consequences diversity and safety dimensions diversity.

2.1 Diversity of technological system change

Technological system diversity can be capture by a two typologies [2]. First typology is related to type of functions potentially performed by a technological system. Four types are considered:

- **Information acquisition**. Automation applied to the sensing and registration of input data.
- **Information analysis**. Automation applied to inferential processes for data extrapolation over time or prediction.

- **Decision and action selection**. Automation applied to definition of alternatives and selection of the suitable one.
- **Action implementation**. Automation executing a set of actions.

Second typology is related to the balance between automation and operator functions for the realization of a task. Ten levels are considered from high-level automation to low level: The computer decides everything, acts autonomously, ignoring the human (10), inform the human only if it, the computer, decides to (9), informs the human only if asked, (8) or executes automatically, then necessarily informs the human (7), and allow the human a restricted time to veto before automatic execution (6), or executes that suggestion if the human approves (5), or suggests one alternative (4), narrows the selection down to a few (3) or the computer offers a complete set of decision / action alternatives (2), or the computer offers no assistance: human must take all decisions and actions (1).

These two typologies capture the diversity of the nature of technological system. This supports the definition of the nature of the change occurring in an organization. Nevertheless, other factors are necessary to describe in order to capture the diversity of new technological change:

- **Purpose**. Qualitative and quantitative reasons that motivates the change (enhancement or reduction of performance criteria, technological innovation, etc.).
- **Justification.** Elements that support the change and its impact.
- **Position**. Situation change in the light of the system: endogenous changes (which occurs within the system studied) or exogenous change (which occurs outside the system under study).
- **Magnitude**. Scope of change within the studied system: changing a dimension of the system or change the overall structure of the system.
- **Timings**. Steps, time, transitions constituting the process of change.
- **Direction**. Comprehensive strategy in which change takes place (link with purpose).
- **Stability**. The change may be permanent, transient on a given state of the environment.
- **Delay**. Delay expected to see the change effect

Those factors allow considering the variety of technological change. Next section is related to the diversity of change consequences.

2.2 Diversity of consequences of change

Technological systems and humans performances in a complex system could lead to different types of consequences related to both their initial goals, specification for technological system and intention for human and interactions and feedback within the environment in which they take place [3][4].

Performance can lead to:

- Positive unexpected benefit usually referred to as serendipity or a windfall.
- Negative effect, occurring in addition to the desired effect of the change.
- Perverse effect (the unexpected adverse effect is greater than the expected beneficial effect)
- Futility of innovation (the more things change, the more they stay the same)
- Threat of achievements (we want to improve society, but only succeeded in removing the freedoms and safety).

Several factors can explain those unexpected consequences:

- Ignorance, it is impossible to anticipate everything, thereby leading to incomplete analysis
- Error, Incorrect analysis of the problem or following habits that worked in the past but may apply to the current situation
- Immediate interest, which may override long-term interests
- Basic values may require or prohibit certain actions even if the long term result might be unfavourable
- Self-defeating prophecy, fear of some consequence drive people to find solutions before the problem occurs, thus the non-occurrence of the problem is unanticipated.

Those concepts support the description of the diversity of potential consequences of a change. Next section us related to the description of different dimensions to be taken in account for considering consequences of change on safety performance.

2.3 Diversity of safety dimensions

This section is related to the description of different safety based dimensions in order to capture the diversity of consequences of a technological change of safety performance. Four dimensions are considerate: Risk dimension, human factors dimension, organisational resilience dimension and inter-organisational dimensions.

Risk is related to the technological system potential failures, their probability and the gravity of their consequences.

Human factors are related to human non-technical skills that can be affected by the technological system: situation awareness, communication, stress, fatigue, decision-making, etc.[5].

Organisational resilience is related to the set of capacities that contribute to the organisation ability to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions[6].

Inter-organisational dimension is related to the set of systems that interact with the organisation and that can be at the origin of unexpected consequences. Such systems

can be legal system, population, clients, suppliers and concurrent, entities situated in the same geographical areas, etc [7].

Diversity of technological system change, of consequences of change and of safety dimension has to be taken in account by a technological assessment process.

Existing approaches neither focus on managing the success of the change without taking in account the safety dimension nor are based on traditional risk assessment methods such as FMECA, THERP or fault tree analysis. Such approaches allow considering a set of consequences but present some limitations regarding, among others things, to consider the complexity of human behaviours, of socio-technical systems and of large-scale socio-technical systems.

Aim of the next section is to describe an integrated framework aiming to integrate actual approaches and extended them in order to capture al the dimension presented.

2.4 The IMPACT method

The IMPACT method aims to provide a set of recommendations based on the analysis of the risks and opportunities of a set of potential consequences identified by the mean of the application of an assessment strategy related to the technological system change studied.

The method is structured with two dimensions. The first one is related to a methodological guideline describing the different steps of the application of the method. The second dimension is related to a toolbox containing different data acquisition processes guidelines and performance indicator assessment guidelines that can be used during the application of the IMPACT method.

2.4.1 IMPACT methodological guideline

The IMPACT method is structured along four phases.

- **Phase 1** *General Outline*. The purpose of this phase is to describe the knowledge necessary to understand the technological change studied and to define a strategy dedicated to the identification of its potential consequences. The strategy is based on the selection of a set of relevant assessment targets.
- **Phase 2** *Consequence identification.* The purpose of this phase is to identify potential consequences of the studied change by the applying the assessment strategy defined in the first phase. The result of this phase will be a list of potential consequences.
- **Phase 3** *Risks and opportunities analysis*. The purpose of this phase is to evaluate the risks and the opportunities associated with the studied change. The set of consequences identified in the previous step is looked at and a list of potential risks and opportunities are defined.
- **Phase 4** *Recommendations for decision-making.* The purpose of the last phase is to define a set of recommendations for the change design and management processes based on the analysis of the set of risks and opportunities identified in the previous step.

In order to support the application of the method a set of methodological guidelines related to on the one hand information acquisition processes and on the other hand performance dimension assessment is proposed.

2.4.2 Impact toolbox

Impact toolbox is constituted of two different methodological guidelines: data collection processes and performance indicator assessment processes. The combination of the two types of processes provides assessment modules to be applied during the consequences assessment phase of the Impact method.

In the actual version of the method three types of data collection processes are available:

- **Risk assessment.** Traditional risk assessment processes based on different types of methods FMECA, HAZOP, THERP, CREAM, etc.
- **Focus group.** Focus Group is an approach that consists in asking a group of person their opinion about their feelings, opinions, beliefs about an idea, a concept, a product, etc.
- **Simulation.** Simulation can be an efficient way to identify consequences of a change on a system. Simple role game or more elaborated simulation using technological facilities such as Bridge, Flight or Crisis management Simulator can be used in order to acquire information about the consequence of a change by, for example, comparing the execution of a given scenario with and without the application if the change.

Four levels of performance indicators are considerate:

- **Risk based consequences**. Consequences related to technical, human or organisational failure modes.
- **Human and organisational based consequences**. Consequences covered by human and organizational factors approaches: Non-technical skills definition and assessment research and development activities (situation awareness, decision-making, communication, teamwork, leadership, stress, fatigue, etc.)[5]; Control performance assessment[8] and risk governance dimension (pre-assessment, management, appraisal, characterization and evaluation and communication) [9].
- **High Reliability Organisation and resilience engineering based consequences.** Consequences covered by research done in the context of safety science: Organizational resilience capabilities (Respond, Learn, Monitor and Anticipate) [6]; HRO abilities of management of unexpected situations (Preoccupation with failure, Reluctance to simplify interpretations, Sensitivity to

operations, Commitment to resilience, Deference to expertise)[10] and Efficiency Thoroughness Trade of model (Work ETTO, Psychological ETTO, and Organizational ETTO) [11].

2.5 Conclusion

Objective of IMPACT framework is to integrate safety dimensions in change management and technological assessment processes.

First methodological guidelines have been developed with a modular approach in trying to integrate different sources of data collections processes and performance indicators.

This framework has been experimented with the assessment of the potential consequences of the use of 3D Chart for navigation functions. A focus group session has been organized with representative of maritime systems and a set of bridge simulation based on a search and rescue mission has been conduct with the use of Stress, Control and Situation Awareness assessment modules.

It's currently experimented with the assessment of potential consequences to the use of UAS and automated threat recognition software for pipeline surveillance. A focus group session has been organized with representative of pipeline surveillance systems and a set of role games has been organized in order to identify stakeholders.

Références

[1] Westrum, R. (1991). Technologies and society. Belmont, California: Wadsworth Publishing

[2] Parasuraman, R., Sheridan, T., & Wickens, C.. A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man and Cybernetics, SMC-30(3),* 286–297, 2000.

[3] Merton, R. K. (1936). The Unanticipated Consequences of Purposive Social Action. American Sociological Review, 1(6), 894-904.

[4] Morin, E. (1990). Introduction à la pensée complexe: Paris: ESF éditeur.

[5] Flin R., O'Connor P., Chrichton M., Safety at the sharp end. A guide to non-Technical Skills, Ashgate 2008

[6] Hollnagel E., Pariès J., Woods D. D., Wreathall J., Resilience Engineering in Practice; Ashgate Studies in Resilience Engineering, 2011

[7] Rinaldi S. M., Peerenboom J. P., Kelly T. K., "Identifying, Understanding and Analyzing Critical Infrastructure Interdepencies", IEEE Control Systems Magazine, 2001

[8] Hollnagel, E., & Woods, D. D. (2005). *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering: An Introduction to Cognitive Systems Engineering*. Boca Raton: CRC Press.

[9] Renn, O., & Walker, K. D. (2008). *Global Risk Governance: Concept and Practice Using the IRGC Framework*. Dordrecht: Springer.

[10] Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the unexpected: assuring high performance in an age of complexity*. San Francisco: Jossey-Bass.

[11] Hollnagel, E. (2009a). *The ETTO Principle: Efficiency-Thoroughness Trade-Off. Why Things That Go Right Sometimes Go Wrong*. Ashgate: Farnham, UK