The standardized generation and the robust filtering of the command as tools of optimization of the mental workload of the systems engineer.

Raphaël Coupat[1&2], Marc Meslay[1], Marc-Axel Burette[1], Alexandre Philippot[2], David Annebicque[2], Bernard Riera[2]

raphael.coupat@univ-reims.fr

[1] IGTE (CES), Direction de l'Ingénierie, Société Nationale des Chemins de Fer Français,

6, avenue François Mitterrand – 93574 La Plaine Saint Denis CEDEX, France

[2] CReSTIC (EA3804), Université de Reims Champagne-Ardenne

Moulin de la Housse, BP 1039, 51687 REIMS Cedex 2, France

Abstract: This paper presents an original approach to standardize the work of electric traction of railway transportation. This approach is developed within an industrial thesis, financed by the SNCF (French acronym for National Society of French Railways) in association with the CReSTIC (Research Centre in Information and Communication Science and Technologies). This approach is composed of two axes. The first axis is the standardized generation of deliverables made by the systems engineers in order to help them keeping their concentration on cognitive task and to avoid repetitive tasks which can lead to mental underload. The second axis is the integration of a robust filter is based on the use of safety constraints within the methodology of standardization. This controller is then constrained by the functional programs, already established and used by the SNCF. The systems engineers can be serene and this filter avoids the stress of decision-making which can lead to a mental overload.

Keywords: control, task-based design, mental workload, standardization process, safety-critical systems, railway transport.

1. INTRODUCTION

The French national rail network (RFN) has to face the competition of the European rail transportation, due to the opening of the market. In order to keep its leadership of the French rail market, SNCF (French acronym for National Society of French Railways) tries to set up innovative solutions improving the productivity. These solutions must not be to the detriment of the safety of installations and persons from which the engineering of the SNCF infrastructure is a guarantor.

In SNCF, the electric traction engineering (IGTE) is in charge of the specification of the equipment of telecontrol, automation and Low Voltage (LV) protections of the Power Supply Equipment of the Electric Lines (PSEEL) market. To improve productivity and performance, IGTE implements solutions harmonizing the working environment of the telecontrol, automation and LV protections design studies, realized on the PSEEL, as specialized project management. Suggested solutions must also be a way to ensure the safety of PSEEL as presented in this article.

The PSEEL are the electrical supply points of the electrified lines, called catenary. The role of the PSEEL is to transform, to supply, even to rectifier in the case of DC supply, the tension of the High-Voltage (HV) network into compatible tension with traction units (1500 V DC or 25 kV AC). These electrical systems, under (very) High-Voltage, are subjected to strict standards of railway safety (EN 50126). The PSEEL are distributed automated systems among which control-command can be done locally but also remotely, in a centralized control station (Gilmore et al., 1989) called Central Sub-Stations (CSS). The human supervisors (Fig. 1) can activate HV devices (switches, circuit-breakers…) since this control room. They are responsible for ensuring the supply of PSEEL under nominal and degraded modes (maintenance of catenary voltage) to ensure safety when working on PSEEL or catenary under national regulations (UTE C 18510) or specific and emergency shutdown in case of electrical danger to persons and properties.

The approach integrates two axes of improvement (Fig. 1). The first one is the standardization, in order to improve the homogeneity of deliverables made by the technical studies. Standardization can also integrate the generation of deliverables (documents, schema...). The deliverables generation allows optimizing the working time of the systems engineers by avoiding them to enter redundant data. The improvement of the working conditions involves a regulation of their mental workload by avoiding the errors consecutive to the mental underload and to the peaks of overload. The second one is the implementation of a robust filter based on safety constraints (Riera et al., 2012) to ensure the safety of persons and PSEEL whatever is the functional control implemented in Programmable Logic Controller (PLC). This control safety filtering should be used to prevent control errors that may be sent from CSS.

This solution is based on the principle of unique data entering, this allows optimizing the workload. The description of the PSEEL in this unique software environment should allow generating all deliverables (documents, programs, wiring diagrams ...). This software solution must be a part of a process of work standardization.

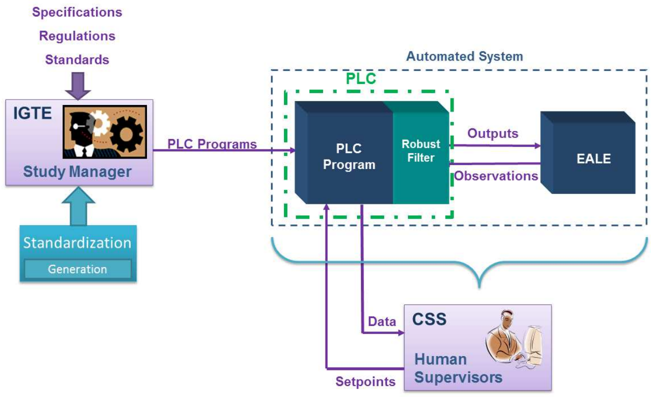

Fig. 1. Application of standardization and robust filter.

Firstly, the paper presents the domain of the electric traction as well as the associated jobs. The mental workload is defined as well as the problems related to this field. In particular the third part speaks about cause and effect of mental underload and overload. The envisaged solutions are presented to counter these mental workload problems thanks to the approach of standardization. Finally, the implementation in the field of Electric Traction is shown.

2. ELECTRIFICATION PROJECT OF PSEEL

Electrification project of PSEEL is divided into several phases (Fig. 2). The project starts with the specifications to define the needs and constraints of the system. This phase is accompanied by the realization of the installation wiring diagrams describing the architecture and related control/command/protections system. Then the systems engineer must study and write the PLC programs, with respect of conception rules established by IGTE. A set of tests procedure, grouped within a testing procedures book, must then be performed to verify and validate the correct operation of the system and programs. Testing procedures (test phase 2) take place in a factory in a first time to validate the wiring and programs. After a correction phase, the testing procedures are realized on site (test phase 3) to validate the full system and electric command of HV devices. Validation of testing procedures book ensures the safety of the system.

The safety of the control system of PSEEL requires introducing the dreaded critical event. This dreaded event is an unwanted command of a device (opening or closing), which would lead to serious consequences and could jeopardize the physical human safety. This is why the field of electric traction is subject to robust constraints of safety of the functioning (EN 50126). The systems engineer is responsible for validating the specifications, testing procedures once completed by realized tests and insuring the integrity of the system. PLC programs implemented by the systems engineer must also be validated during tests phase.

The design rules of the programs are described within the principles of PSEEL automation (Fig. 2) through GRAFCET (IEC 60848) specifications describing the sequential HV functioning of devices.

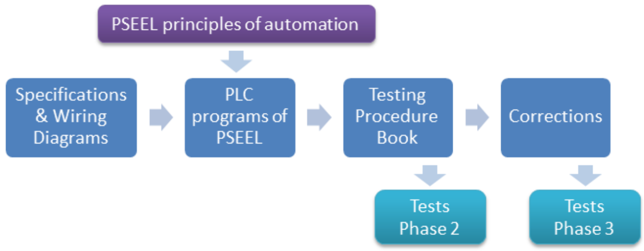

Fig. 2. Division of the project phases of electrification.

The work of design and study of the PSEEL, realized by the systems engineers, requires a hard intellectual activity during the entire project and to avoid mistakes. This concentration can be altered by several factors. The most compelling element of concentration alteration, reducing the concentration and therefore the effectiveness of the systems engineer, is the plurality of the current projects which he/she has to realize in a limited time. Indeed a number of hours is allocated to each task of a project, depending on the complexity of the structure of the PSEEL. The concept of deadline may cause additional stress (Sargent and Terry, 2000). Within the project workflow, the multiplication of the realization computing tools of the various tasks does not help the systems engineer to optimize his/her working time. The tool switch can lead to a loss of information and errors while copying. Moreover, a relationship was shown between the multiplication of resources and working memory (Wickens et al., 1998) which can lead to mental overload (Young and Stanton, 2001).

This plurality of tools, needed to provide various deliverables (documents, programs, wiring diagrams ...), also causes multiple data entering of the same information about a project. This repetitiveness of action, besides being source of error and a waste of time, harms in the concentration as well as in the interest which the systems engineer feels in his work by the lack of valuation and gratitude. Mental workload is therefore reduced, and mental underload comes (Stanton et al., 1997). These notions of mental workload are defined in the third part, dealing with mental workload. Furthermore, the systems engineers are a team and work separately, which can lead to different assessments of the set up principles.

The cognitive task of studying and designing PSEEL could be assisted to avoid mental overload due to the stress of decision-making. This mental overload, to be ensured that the critical event does not occur, is only undergone by the systems engineer who studies and designs the system to insure its safety. This assistance to the systems engineer would provide an improved safety to system and persons. Indeed, a mental overload can lead to a risk of control error and jeopardize the safety of the system (Millot, 1987). It is essential that they have a real Situation Awareness (SA) in which the system is. To assist operators in their missions, it is possible to develop a tool to send efficient information to the system engineer (Fig. 3) from the robust filter in case of violated safety constraints. The purpose of this assistance, in addition to the safety provided by the filter would be to limit the stress of the system engineer.

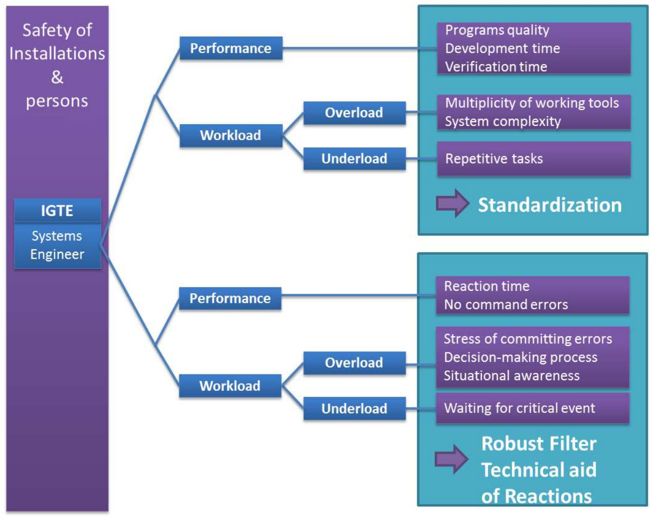

Fig. 3. Representation of the solutions proposed to increase performance and mental workload.

3. MENTAL WORKLOAD

The mental workload (ISO 10075) in the automation field is a major concern since a few years. This persistent notion has never been completely surrounded and is a part of the social debate related to work intensification (Askenazy and Caroli, 2003). It is defined as the quantitative or qualitative measure of the level of activity required to perform a specific work (Sperandio, 1988). In other words, the concept of mental workload is defined fundamentally in terms of the relationship between the supply (resources) and demand (requirements) (Wickens, 1984). The workload is a complex concept which use has been extended to many areas of psychology and ergonomics (Richard, 1996). It indicates the consequences of the execution of the task on the operator (in this article the operator represent both the systems engineer and the human supervisor). The task itself and its constraints are included under the name of requirements of the work. The study of workload connects the physical and the mental aspect of the operator, considering that his physical condition impacts his mental tolerance to the effort (Cnockaert and Floru, 1991). The effort corresponds to the cost of mental work, so appearing as the result of the mobilization of all the mental functions involved by the operator to realize a task (Lancry and Lammens, on 1998).

When the cost of mental work is excessive in relation to the tolerance of the operator, it appears an overload situation. Overload appears in a situation such as the body cannot handle all the information available, causing a high number of errors. It harms in the performance of the operator (Fig. 4). On the contrary, when the body works below its possibilities, it is confronted with a phenomenon of underload. That risks provoking a falling asleep of the operator (Sperandio, 1988). This state can be classified as the category of hypovigilance, mostly observed in the repetitive tasks (François, 1989).

Mental underload decreases the performance of the operator (Fig. 4), as the left side of the performance curve shows that. Fig. 4 shows the relation between the mental workload and the performance of the operator, it shows well that extremes provoke a reduction in the performance. Indeed, after an interesting work requiring few intellectual abilities, it is more difficult for anyone to start a task requiring a high level of cognitive reflection and concentration (Young and Stanton, 2008). This is especially true in the field of automation of complex safety systems like PSEEL (Amalberti, 2001). This quick level change of necessary concentration can be source of human errors. Human error must be minimized in achieving safe systems. Although errors can be detected during validation tests, it is better to inhibit them upstream.

Fig. 4. Inverted-U curve showing the influence of workload on performance.

To improve the performance of the team to design the electrification projects, the homogenization of documents and deliverables seems to be an effective solution. Indeed, through the standardization, it is possible to improve performance and quality by defining rules in order to make the reading of a project easier for everyone. This article will also show that the safety aspect of the approach, improves mental workload of the systems engineers.

4. STANDARDIZATION PROCESS

Standardization of a job is a process requiring the domain know-how and having a global vision (job expert). It is therefore natural that the first phase of this approach is a study of all the principles used by the job to understand the know-how. Indeed, the workflow methodology followed by the systems engineers is composed of many tasks (Fig. 2). Each accompanied by deliverables that would be interesting to standardize.

4.1 System modelling

The approach of standardization is based on an object view of the complex system. Indeed, by decomposing the system, the PSEEL, in sub-systems (sSys) (Transformation Group, Track Feeder, Common …) (Fig. 5), a first view of the subassembly PSEEL can be done. This view is used to distribute the system control. This division is used as well to distribute the components of each deliverable by sSys. Then each sSys can be decomposed into Elements of the System (ElSys) (Circuit Breaker, Switch …), which correspond to "objects" of the system (Fig. 5). Each object can then be associated with different deliverables components.

Thus it is possible to reconstruct the project deliverables from a description of the system containing the sSys itself compound of ElSys. The detailed description can then generate all deliverables following the existing project workflow. The generation avoids a multiple data entering in multiple deliverables, which may cause a feeling of dullness

(Sperandio, 1988). This unique description can then focus the attention of the systems engineer and optimize the curve of his mental workload. The configurable description adds safety in the project generation process. Indeed, during the description, a consistency check is made to prevent the inconsistent data entering. The information is then visible by the systems engineer so that he can correct his own error. The consistency check is based on the relational database model of the system corresponding to the object model.

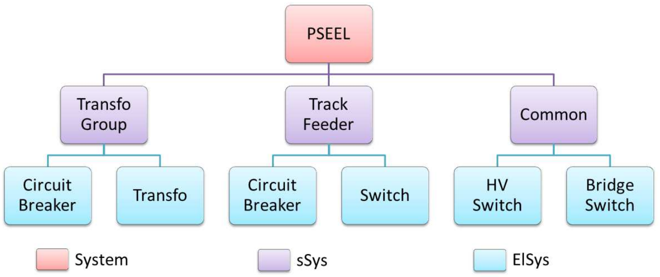

Fig. 5. Object modeling of a PSEEL.

4.2 Generation of deliverables around mental workload

Generation of deliverables from the unique description made by the systems engineer requires a second reading. This cognitive task asks for more concentration of the systems engineer because it is about the documents validation which he/she would have to write previously (but not anymore). This phase of proofreading also allows the systems engineer to have a critical look on the generated elements. This feedback allows improving the generation. He/she must be concentrated to analyze the lacks and complete the generated elements. This task requires, also, a significant concentration of the systems engineer. He/she has to complete at the same time the deliverables but also the programs for the ElSys which were not able to be defined during the description.

This new workflow eliminates the mental underload phases, replacing them by cognitive phases which the sequence avoids the mental overload. The unique data entering in a software environment allows the systems engineer to stay focused and not to lose in performance. Indeed, the information contained in the deliverables may be duplicates, systems engineer must then write the duplicated information several times. This monotonous repetitive work makes the systems engineer work unattractive. That is a source of error and, as mentioned above is also a source of mental underload.

The concentration of the systems engineer is then focused on a new task, in which he/she has to describe only once all the parameters of the design project of the PSEEL to generate the standardized deliverables. When the standardized deliverables are generated, the systems engineer must implement all his/her know-how to design and compute the elements that are not standard. Indeed, the variety of elements (ElSys) makes impossible to have a complete standardization. Each installation has particularities of which the systems engineer must take care. All the systems engineers will use this solution, what will therefore make all projects, more homogenous and more easily understandable by all.

4.3 Generating a quality PLC code

The main interest of this standardization approach is the automatic PLC code generation. Fig. 6 shows the steps of this approach which will be detailed in this article.

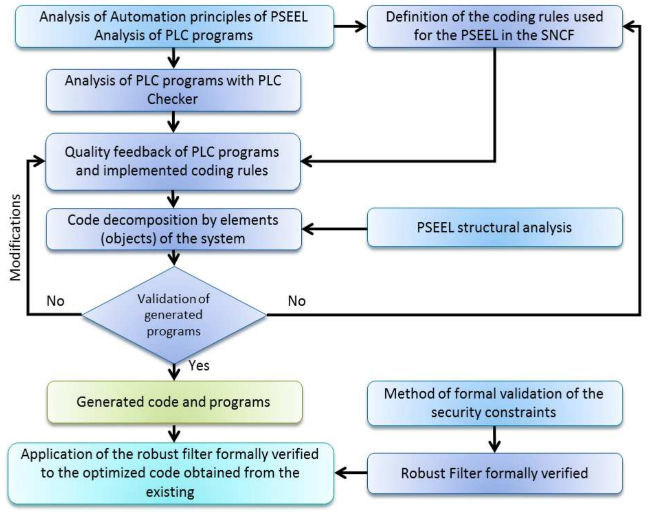

Fig. 6. Decomposition of the Standardization approach.

Before the implementation, it is necessary to define requirements through a specification. Fig. 5 seen above shows the object oriented aspect of our generation process. To build the generation model, input data are necessary:

- “Who?” Who are the objects that will make up the model?
- “What?” What is the functionality (attributes and services) object will provide?
- “Where?” Where will the object be controlled as the system is distributed ? (which PLC?)
- “How?” How to organize the final model in coherent way ?

To answer these questions, an analysis phase of the programs and systems principles is necessary. From this analysis, the standardization process starts with a normalization phase of the computing rules used by the SNCF. It is then necessary to use the object modeling of the system to assign the standardized code to each ElSys. The normalization is done from the expertise and feedback from studies and analysis programs made with PLC Checker (www.automationsquare.com/plc-checker.html). This tool automatically analyzes PLC programs and verifies, in an exhaustive way, their conformity with generic rules (ISO 9126). This standard describes the requirements of:

- Readability (comments, variable naming),

- Reliability (all inputs are read, all outputs are written, all defects are evaluated, all sections are present and in the specified order),

- Modularity (no dead code and uncalled subroutine, variables are properly handled and in the right place).

The use of this tool allows IGTE to assure the respect of the generic computing rules but also of the specific rules of Electric Traction field. Indeed, it is possible to define additional specific rules to verify the consistency of the programs. A specific rule to IGTE is the implementation of

GRAFCET in the PLC programming environment in SFC (IEC 61131-3). GRAFCET allow a formal description of the desired functioning of the system. The SFC programs of all the projects follow the same structure allowing any systems engineer to understand the program thanks to comments and to naming which have to follow the described rules.

Thanks to PLC Checker, it is possible to objectively analyze the programs quality to have an experience feedback on them. The results show no errors of reliability in the systems engineers programs. Nevertheless, the results show disparities in the code of the systems engineers. For example, they are not subject to strict naming rules. That is why a variable representing a specific event may have different names depending on the program. Information about modularity concerning the existence of unreachable and dead code or uncommented code also appeared to the analysis.

To generate a quality PLC code, it is necessary to harmonize the programs before, to have typical programs. These typical programs are based on the principles of automation described by IGTE. The process of standardization is thus ideal to harmonize the programs and improve their quality. It is then necessary to break up the system starting from the structural analysis of the system in order to assign to each ElSys the standardized code which corresponds to it. As we explained through the fig. 5, each elSys is part of a sSys. The system being distributed, each sSys is controlled by a PLC, specifically assigned to the sSys, in order to ensure the greater system reliability and availability. Thus the elSys, children of same a sSys are controlled by the same PLC. For example, two sSys insuring the same function are controlled by two dedicated PLC. Their elSys are controlled by a PLC dedicated to the parent sSys. So if one of the sSys breaks down, the other still ensures the functionality by redundancy.

The generated programs can be divided into three steps:

1. Beginning PLC cycle:
   - Initialization of the variables,
   - Reading of the inputs state,
   - Reading of the variables on the network,
   - Observers construction,
2. Control programs of the devices:
   - Sequential control of the devices,
   - Checking of the orders coherence,
3. End PLC cycle:
   - Writing of the variables on the network,
   - Writing of the outputs.

The programs of steps 1 and 3 are attached to the PLC in charge of a sSys, they follow a standardized structure and are generated according to the type of sSys and of the elSys children. Whereas the programs of step 2 are only related to the elSys controlled by the PLC. For example, each Transfo Group (TG) is controlled by a dedicated PLC. Each TG PLC program is so composed of step 1 and 3 sub-programs. Each TG is composed of a circuit breaker, of a quick break switch but also of HV switches or other devices. So the step 2 sub programs are different according to ElSys of this sSys.

From the standard code assigned to elements of the PSEEL, it is possible to generate the code of the automation. It is then necessary to check the validity of the generated code and its quality. If the code is validated, then the tool can be used by the systems engineers to design PSEEL.

Finally, the last phase of the approach is the implementation of the robust filter based on safety constraint on the same principle of affectation and decomposition according to the structure of the PSEEL.

5. SAFETY BY ROBUST FILTER OF CONSTRAINTS

In the approach described in Fig. 6, the last step is to add a safety layer with a filter of Boolean constraints formally verified by using a model-checker. The quality and the rigor of control-command synthesis realized by a systems engineer depend only on his/her skills and experiences. System safety is ensured by the robust filter regardless of the implemented control-command. Indeed, ensuring a formal safety to automated systems is a scientific challenge that issues important industrial stakes. The interest of the robust filter is to insure systems engineer that he/she will not interfere with system and human safety. So he/she can be serene and it avoids a state of stress which can lead to a mental overload.

A methodology has been described by (Marangé et al., 2010) to get a robust filter formed by a set of safety constraints formally verified from a dysfunctional analysis of the system. This check is done through the model-checker UPPAAL (Behrmann et al., 2002), allowing the system modeling then the formal verification of system properties and proposed logical constraints. Safety constraints are expressed as a monomial (product of logical variables, Π form) which is a logical function of the inputs / outputs of the PLC and any possible observers (function of inputs) to compensate the lack of observability of the system. The robust filter is implemented at the end of the control-command program in the PLC.

Although this formal approach requires the intervention of an expert of the system, combined with the standardization process, it allows to strengthen the safety of the elements of the system without complicating the work of systems engineers. This work of elementary decomposition of the safety constraints must not evolve. Only the functional part of elements may need to be modified. The safety part must be the same in anytime. That is why the interest to insure the safety of the ElSys and of the global system, thanks to the formal filter, whatever is the implemented command in the PLC seems obvious.

6. APPLICATION ON PSEEL

The process of standardization and safety presented in this article demonstrates an interest at several levels of the life cycle of a PSEEL.

Indeed, during the design phase (Fig. 7a), the generation avoids repetitive tasks due to the data entering of redundant information. The solution of generation allows to refocus the concentration of the systems engineers on the cognitive tasks and so to avoid mental underload. The standardization approach also prevents mental overload, due to the proliferation of computing supports, by integrating a software environment based on a unique data entering.

The robust filter can inhibit command errors of an operator, the sending of an erroneous command will be filtered by the safety constraints implemented in the robust filter. This kind of error can occur when the operator is mentally overloaded, in case of simultaneous incidents. This additional safety helps to decrease the stress suffered by the operator due to the decision-making in a limited time (Fig. 7b). The inhibition of a command sent by the operator will have the effect of awakening the human supervisor vigilance (Hancock and Verwey, on 1997). This effect can be beneficial when the human supervisor undergoes an overload peak after mental underload phase due to the waiting for an event.

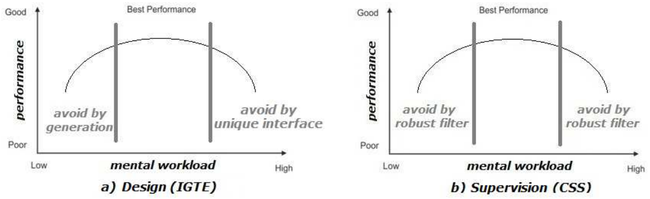

Fig. 7. Influence of various benefits on PSEEL life cycle.

7. CONCLUSIONS

This article shows the interest of the approach followed by the SNCF, to standardize and generate all the deliverables, to improve the level of performance that can be achieved at the end of the project. The axis about safety, represented by the robust filter, can also improve the performance and mental workload through preventing operating errors.

Track development of the approach is the implementation of a feedback to the CSS when a safety constraint is violated. This feedback would allow meaningful interaction between the human supervisor and the robust filter. Nevertheless, this solution cannot be applied at the moment for technical reasons. It is currently not possible to measure the actual effect of our approach on the life cycle of the PSEEL. To bring these results, it is necessary to wait to have an experience feedback over a significant duration to be able to compare with existing systems.

ACKNOWLEDGEMENTS

The authors thankfully acknowledge the support and the interest from SNCF. We are indebted the IGTE members for their strong experience in PSEEL work.

REFERENCES

Amalberti, R. (2001). *La conduite de systèmes à risque*. Paris

Askenazy, P., and Caroli, E. (2003). *Pratiques innovantes, accidents du travail et charge mentale*: résultats de l'enquête française sur les Conditions de travail. Pistes, 1 (5), 1-30.

Behrmann G., Bengtsson J., David A., Larsen K.G., Pettersson P., Yi W., 2002. Uppaal implementation secrets. *7th International Symposium on Formal Techniques in Real-Time and Fault Tolerant Systems.*

Cnockaert, J.C., and Floru, R. (1991). *Introduction à la psychophysiologie du travail*. Nancy: PUN.

EN 50126. *Applications ferroviaires* - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) (2000).

François, M. (1989). *Ergonomie des postes de contrôle qualité; étude bibliographique*. Cahiers des notes documentaires, 137, 595-606.

Hancock, P. A., and Verwey, W. B. (1997). Fatigue, workload and adaptive driver systems. *Accident Analysis and Prevention*, 29(4), 495-506.

IEC 60848. *Specification language* GRAFCET for sequential function charts Ed. 2 (1999).

IEC 61131-3. *Programmable controllers* - Part 3: Programming languages Ed. 2 (2003).

ISO 9126. *Software engineering*-Product quality Ed.2 (2001).

ISO 10075. *Principes ergonomiques concernant la charge de travail mental* -- Termes généraux et leurs définitions (1991).

Lancry, A., and Lammens, J.M. (1998). Étude différentielle des fluctuations de performances à une tâche complexe au cours de la journée. *Le Travail Human*, 61 (2), 153-169.

Marangé P., Benlorhfar R., Gellot F., Riera B., 2010. Prevention of human control errors by robust filter for manufacturing system, *11th IFAC Symposium on Analysis, Design, and Evaluation of Human-Machine Systems*, France.

Millot P, (1987). Coopération homme machine dans les tâches de supervision des procédés automatisés, thèse de doctorat.

Richard, J.-F. (1996). Faut-il revoir la notion de charge mentale ? *Psychologie Française*, 41 (4), 309-312.

Riera, B., Philippot, A., Annebicque, D., Gellot, F. (2012). *8th Symposium on Fault Detection*, Supervision and Safety of Technical Processes (SAFEPROCESS 2012), Mexico.

Sargent, L.D. and Terry, D.J. (2000). The moderating role of social support in Karasek's job strain model. *Work and Stress*, Vol. 14, No. 3, p. 245-261.

Sperandio, J.C. (1988). *Ergonomie du travail mental*. Paris.

Stanton, N. A., Young, M., and McCaulder, B. (1997). Drive-by-wire: The case of driver workload and reclaiming control with adaptive cruise control. *Safety Science*, 27(2/3).

UTE C 18510. Operations on electrical work and installations and in an electrical environment - *Electrical hazard prevention.*

Wickens, C. D. (1984). Processing resources in attention. In R. Parasuraman and R. Davies (Eds.), *Varieties of attention* (pp. 63-101). New York: Academic Press.

Young, M. S. and Stanton, N. A. (2001). Mental workload: theory, measurement, and application. In W. Karwowski (Ed.), *International encyclopedia of ergonomics and human factors*: Volume 1 (pp.507-509). London: Taylor and Francis.

Young, M. S. and Stanton, N. A. (2008). Attention and automation: New perspectives on mental underload and performance.