Standardization and safety control generation for SNCF systems engineer

Raphaël Coupat[1&2], Marc Meslay[1], Marc-Axel Burette[1], Alexandre Philippot[2], David Annebicque[3], Bernard Riera[2]

raphael.coupat@univ-reims.fr

[1] PSIGT-TE (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

[3] CReSTIC (EA3804), IUT de Troyes, 9 rue de Québec, BP 396, 10026 TROYES, CEDEX, France

Abstract: This paper presents an original approach developed within an industrial thesis, financed by the SNCF (French acronym for National Society of French Railways). The aim is to standardize the work of electric traction of railway transportation. This approach is composed of two axes. Firstly, a standardized generation of deliverables is done to help the systems engineers keeping their concentration on cognitive task and to avoid repetitive tasks which can lead to mental underload. Secondly, a robust filter based on the use of safety constraints is integrate. This controller is then constrained by the functional programs, already established and used by the SNCF. The system safety is insured by the robust filter which has been formally verified by model-checking.

Keywords: Power and Energy Systems, Robust Control Design, Social Impact of Automation, Safety-Critical Systems, Railway Transportation Systems.

1. INTRODUCTION

The French national rail network 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, PSIGT-TE 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 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 (S11, log C) 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. 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.

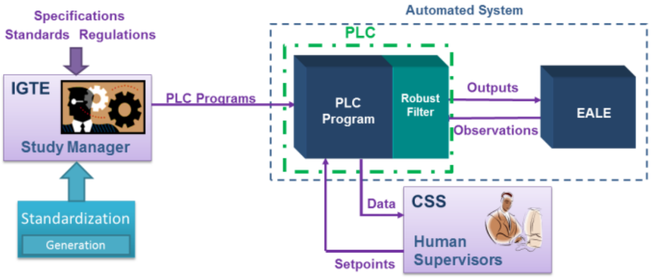

Fig. 1. Application of standardization and robust filter.

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.

Firstly, the paper presents the domain of the electric traction as well as the associated jobs. Section 3 briefly defines the mental workload. The exhaustive definition has been done in (Coupat *et al*, 2013). The envisaged solutions are presented to counter these mental workload problems thanks to the approach of standardization, in section 4, and to the robust filter implementation in section 5. Finally, the implementation of those solutions in the field of Electric Traction is presented.

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 (tests 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 (tests 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.

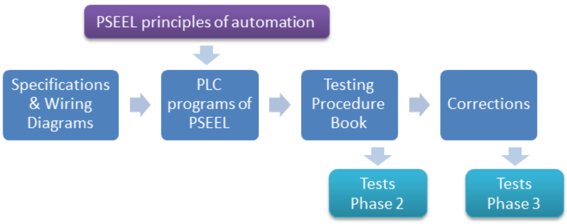

Fig. 2. Division of the project phases of electrification.

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 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 of this paper, 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.

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 (Millot, 1987). The task itself and its constraints are included under the name of requirements of the work. 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) (Fig. 3).

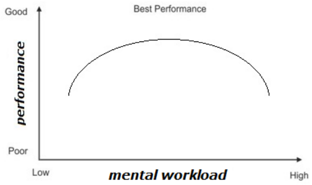

Fig. 3. Inverted-U curve showing the influence of workload on performance.

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. 4), 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. 4). 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. 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.

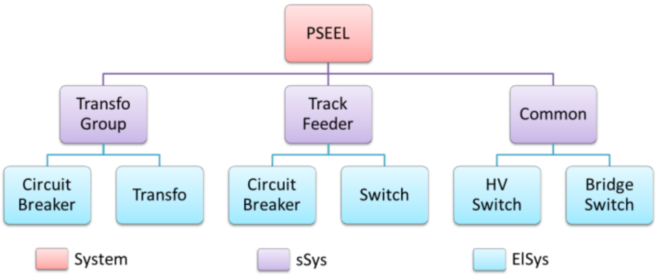

Fig. 4. Object modeling of a PSEEL (system decomposition).

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.

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 Generation of a quality PLC code

The main interest of this standardization approach is the automatic PLC code generation. Fig. 5 shows the steps of this approach which will be detailed in this article.

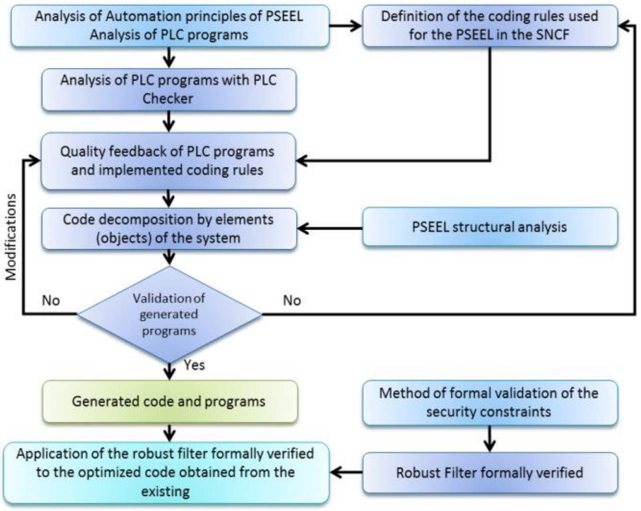
Analysis of Automation principles of PSEEL
Analysis of PLC programs
Definition of the coding rules used for the PSEEL in the SNCF
Analysis of PLC programs with PLC Checker
Quality feedback of PLC programs and implemented coding rules
Code decomposition by elements (objects) of the system
PSEEL structural analysis
Modifications
No
Validation of generated programs
No
Yes
Generated code and programs
Method of formal validation of the security constraints
Application of the robust filter formally verified to the optimized code obtained from the existing
Robust Filter formally verified

Fig. 5. 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[1] . This tool automatically analyzes PLC programs and verifies, in an exhaustive way, their conformity with generic rules (ISO 9126). 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.

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. 4, 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 sSys and ElSys children types. On the contrary the step 2 programs are only related to the ElSys controlled by the PLC.

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. 5 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 Failure Modes and Effects Analysis (FMEA) 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 (Fig. 6). 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.

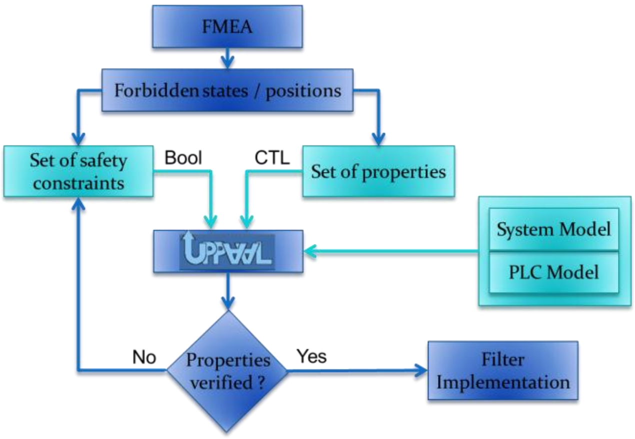

Fig. 6. Safety command filter synthesis.

The robust filter is implemented at the end of the control-command program in the PLC. It is then possible to verify formally if the set of safety constraint is necessary and enough to ensure the system safety thanks to UPPAAL. The devices command model and the system evolution model are not enough to simulate the system. It is necessary to define the system model and the PLC cycle model. The PLC Cycle Model (Fig. 7) is decomposed in ordered sub tasks.

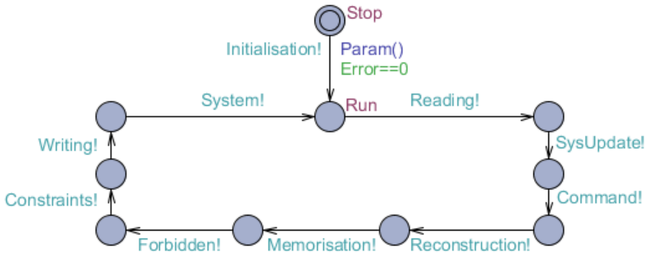

Fig. 7. PLC Cycle Model with Uppaal.

[1] www.automationsquare.com/plc-checker.html

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

One of our proposals is to define the constraints not from the FMEA but from the testing procedures book. As we said before, verification and validation of the system and programs correct operation are ensured by the testing procedures book. Those tests are realized on each PSEEL of the RFN. We assume that it is not a formal definition way. Nevertheless this set of safety constraints, if it is well written, ensures that the testing procedures book we will be respected and passed. The tests phases are not formal but it has the interest of the experience feedback. Indeed, after dozens years of exploitation, the PSEEL safety has always been ensured. The experience feedback is the first thing to take in the account, establishing the set of constraints from the testing procedures book and so on the experience feedback, permit to ensure the safety rules already defined by the SNCF.

For example, in a TG, the HV Switch (HVS) must not be closed if the TG Circuit Breaker (TGCB) is not open. The HVS must not be opened if the TG Circuit Breaker (TGCB) is not open.

That can be written[2]:

(CSS1) CCHVS . NOT(soTGCB) = 0

(CSS2) OCHVS . NOT(soTGCB) = 0

On the contrary, the Snap Action Switch (SAS) of the TG can be opened in charge, so no constraints are applied. But the SAS must not be opened if the TGCB is not open. That can be written:

(CSS3) OCSAS . NOT(soTGCB) = 0

With those three constraints the filter ensures that no erroneous command or order can be sent either to the HVS or to the SAS.

During the PLC first cycle, an initialization step is necessary to configure the studied system. After this configuration step, the normal cycle starts with the reading of the system information by the PLC inputs. The command models are then able to evolve and the PLC outputs are updated with the new command defined. After this commands, observers are constructed, in particular inputs and outputs rising edge and falling edge which are very useful. After the observers' construction and memorization, the robust filter operates to verify that the proposed PLC outputs are not going to violate any safety constraints. If a safety constraint would be violated, the default output would be changed to stay in the system safety space of functioning. When the set of constraints is respected, the outputs are written and the system model is updated to take in the account the new position of ElSys after one PLC cycle in order that the system model evolving is considerate by the next inputs reading.

The PLC cycle is decomposed to obtain a model that is the nearest from the system reality. The devices command model (Fig. 8) has been defined with the possibility of one transition by PLC cycle.

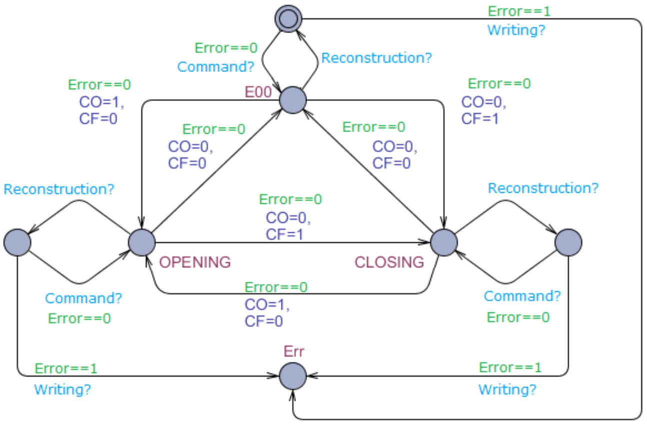

Fig. 8. Switch Command Model with Uppaal.

The devices state model includes a transition state during which the device position is not known (Fig 9): so = sc = 0. The opening and closing movement are considerate as courses during PLC cycle.

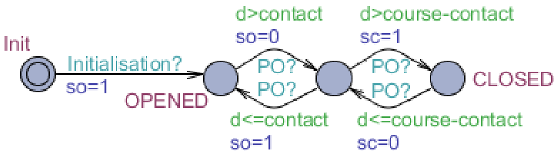

Fig. 9. Switch Evolution Model with Uppaal.

The implementation of those models under Uppaal allows the formal verification of the properties which must be respected by the system. To verify the properties, Uppaal uses the CTL logic (Clarke, E. *et al.* 1986) and try to find a way showing that properties are not verified. If the system safety is ensured, then the robust filter can be implemented at the end of the PLC cycle.

7. CONCLUSIONS

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. 10a), 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

[2] OC: opening command CC : closing command
so : signal of opened state sc: signal of closed state

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. 10b). The inhibition of a command sent by the operator will have the effect of awakening the human supervisor vigilance. This effect can be beneficial when the human supervisor undergoes an overload peak after mental underload phase due to the waiting for an event.

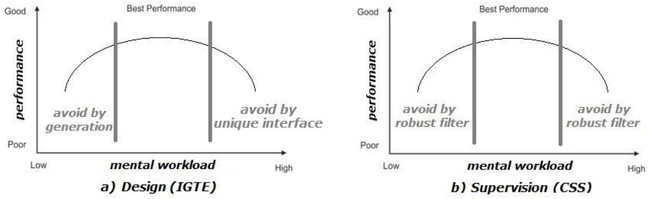

Fig. 10. Influence of various benefits on PSEEL life cycle.

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 PSIGT-TE members for their strong experience in PSEEL work.

REFERENCES

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*. Springer-Verlag London, UK 2002: 3-22.

Clarke, E. M., Emerson, E. A., and Sistla, A. P. (1986). "Automatic verification of finite-state concurrent systems using temporal logic specifications". *ACM Transactions on Programming Languages and Systems* 8 (2): 244–263.

Coupat, R., Meslay, M., Burette, M. A., Philippot, A., Annebicque, D., Riera, B., (2013). Standardized generation and Robust filtering for optimization of the mental workload of the systems engineer. *12th IFAC Symposium on Analysis, Design, and Evaluation of Human-Machine Systems* (HMS 2013), Las Vegas.

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

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 Humain*, 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* (HMS 10), France.

Millot, P. (1987) Coopération homme-machine dans les tâches de supervision des procédés automatisés. *Thèse de doctorat*, Université de Valenciennes.

Moeschler, J. 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, pp. 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. *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*: Vol. 1, pp.507-509. London: Taylor and Francis.