Role of supervision systems in railway safety

F. Belmonte, J.-L. Boulanger, W. Schön & K. Berkani
Laboratoire Heudiasyc, Université de Technologie de Compiègne, France

Abstract

The new generation of supervision systems in industry can achieve operation from display process variables to all automated control where the human is just the monitoring automaton. In the railway specific industry, supervision is organised in switching zones and aims to be centralised in an Integrated Control Centre. Such centres implement integrated and computer based systems that perform train protection, train operation and supervision. Thus railway dispatchers using supervision have their tasks considerably simplified. Although considered today as not safety critical, railway supervision systems can contribute to safety in some scenarios where an appropriate decision of a supervision operator could notably reduce the severity of accidents. That is in particular the case for residual scenarios (intervention of maintenance teams on the tracks, manual operation of trains not protected by train protection system, coupling/uncoupling, emergency requiring the stopping and evacuation of a train etc) only covered by procedure, thus requiring human intervention by a person supposed correctly informed on the state of the system, thanks to the data provided by the supervision system.

Keywords: supervision, automatic train control, safety, human factor.

1 Introduction

Whatever the degree of human presence aboard trains, all railway lines have however a system which centralizes for operators of a central room, as well the operations of traffic control (signalization, traced routes etc.) as operations of traffic regulation. Formerly analogical, today technology is becoming numerical. Therefore, it is now possible to generalize the centralization of many functionalities formerly carried out locally by operators on-site (signals and

WIT Transactions on The Built Environment, Vol 88, © 2006 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR060131

switching devices handling, traction energy management, disturbance management, public places monitoring). This technological development improvement must be accompanied by an evolution of operator's culture. On the one hand, the increasingly frequent use of numerical technology in safety functions requires rigorous process development. On the other hand, the activity of human operators changed much: operators on-site (drivers, pointsmen) are becoming more and more supervisors of automats. They must apprehend, analyze the remote situation and as far as possible often act with the help of remote controls.

This paper is structured as follows. Section 2 presents a general overview of supervisory control, the definition of supervision of railway network, and how the supervision systems are implemented and deployed. Section 3 deals with safety concepts and implementation in automatic train control systems. We explain how safety could be improved with the help of supervision systems. Section 4 presents our supervision platform which is installed in University of Compiègne. Human behaviour experiment will be performed using this platform.

2 Supervisory control/command theory

Industrial process supervision covers a wide range of applications, from simple control to complex and heterogeneous system control. The aim of this section is to introduce basic definitions about supervisory control system. They define the context of our approach.

2.1 Definitions

Originally, the term supervision refers to the human interaction between a superior and his subordinates. Dictionary [8] defines supervision as monitoring and overseeing a task without going into particulars.

In control and automatic context the definition of supervisory control is the control and the monitoring of a system including, where appropriate, those operations which ensure reliability and safety. In addition, "Automation dictionary" gives the following meanings to supervision control:

1. "Control in which the control loops operates independently subject to intermittent corrective action". For example, the corrective action can be set point changes by an operator or another external source;
2. "A term used to imply that a controller output or program output is used as an input to other program, e.g., generation of set points in cascade control systems", used to distinguish from direct digital control.

There are two major models of supervision from scientific literature. Supervisory control theory is the first of them. This model was introduced by Ramadge and Wonham [4] from automatic theory domain. It consists of analyzing discrete events control systems in a formal manner. Railway Traffic could be reduce to discrete event control system. The process is modelled as a state-transition structure, labelled a Finite State Machine, in which transitions are labelled as controllable and uncontrollable. Control actions are exerted upon the

process in feedback mode by another FSM termed supervisor that disables controllable transitions in order to satisfy given behaviour specifications. In other words the supervisor disables process controllable transitions in such a way that it restricts the process behaviour to a subset of all the possible trajectories.

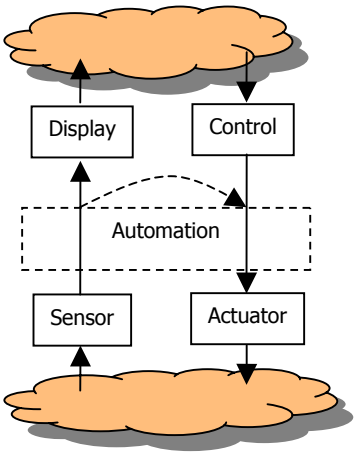

Figure 1: Sheridan supervisory control model.

Another model, even more generic was introduced by Sheridan [1], his concept of human supervisory control is depicted in Figure 1: by five main tasks. In supervisory control, a human operator monitors a complex system and intermittently executes some level of control on a process, always acting through some automated agent. During supervisory control, an operator plans an activity and instructs it to a computer. A human checks if the actions are executed and intervenes in case of computer failures. Finally, the human learns from the experience. The interrelationships between the five supervisory tasks are characterized by three loops (see Figure 2:). The inner loop is the monitoring where observations lead to further detections and diagnostics. The intermediate loop relates operator interventions to reprogramming or modifying the computer system to follow new goals or reach new states. The outer loop feeds the latest process knowledge and experience from learning back to planning. The three loops operate on different time scales. The inner monitoring loop is executed frequently while modifications of process goals (the intermediate loop) are done less frequently. Finally, the overall process plans and goals are changed over relatively long time intervals.

Supervisory control is that a human operator is intermittently giving a command and receiving information from a computer that itself is an automatic controller to a given system [1].

Implementation of supervisory control system are based on SCADA systems [3], the next section presents briefly their principal characteristics.

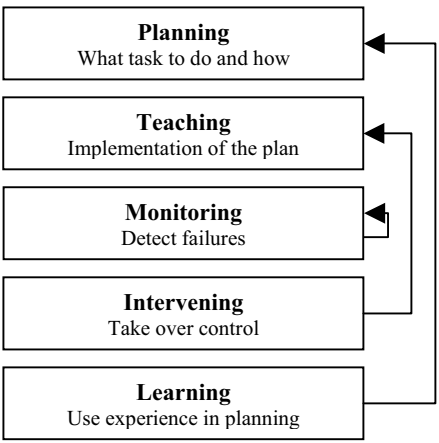

Figure 2: Five tasks in supervision (from Sheridan).

2.2 SCADA

SCADA is an acronym that is formed from the first letters of the term "supervisory control and data acquisition". SCADA is the implementation of supervisory system.

At the centre of SCADA system, the operator accesses the system by means of an operator interface device. The operator consoles functions as the operator's window into the process. It consists of a video display unit (VDU) that displays real-time data about the process and a keyboard for imputing the operator's commands or messages back to the process. Other cursor-positioning devices, such as a trackball, mouse, or touch screen may be used. If the system is very simple, it may be sufficient to have a set of annunciator windows that mimic the condition of the remote process. Often, an audible signal for alarms will be included. The operator interfaces with the master terminal unit (MTU), which is the system controller. It can monitor and control the field even when the operator is not present. It does this by means of a built-in scheduler that can be programmed to repeat instructions at set intervals. MTU must communicate with remote terminal units RTUs that are located away from the central location. A SCADA system may have as few as one RTU or as many as several hundred. RTU communicates with RTUs using the communication network (Radio, serial communication, Ethernet, etc.).

SCADA systems (see Figure 3:) consist of three functional components: communications equipment, remote terminal units and master terminal unit. RTU gathers information from field and centralise this through communication network to MTU. Then MTU treats this information and displays them to operator through Human Machine Interface. MTU also achieves tasks (automation tasks) but always present information (treated or direct from field) to operator.

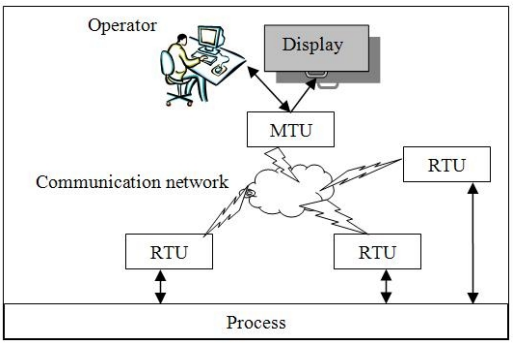

Figure 3: SCADA system.

3 Railway supervision

3.1 Integrated Control Centre

Railway supervision system includes 3 hierarchical levels: (1) Route control level includes field control and commands as route setting, train control and protection functions. (2) Traffic flow control level insures conflict solving, and time graph monitoring functions. Finally (3) the highest level performs management and planning tasks. There are several implementations of the three levels. One could separate each level in three control rooms. This is the case for large railway networks with a lot of inter connexions. These kinds of networks are segmented in switching zones where signal boxes achieve route control level. Generally, centralized traffic control (CTC) centre gathers several switching zones. CTC achieve the level 2 of supervision (traffic flow control). Finally, coordination control centre manages the entire network. It could be international, national or regional organisation. Other implementations centralise the three level of supervision in a unique centralised room called operation control centre (OCC). This is the case for metro and urban railway network. Indeed, such networks are characterized by their unique line and their rare connections with other networks.

These kinds of implementations could be explained by the technology used until today that not permitted to integrate very large network control in a single room. With the emergence of high intensive computerised systems in railway supervision, operational company use more and more integrated control centre (ICC) (see Figure 4:). ICC could gather operation and control on the three levels of supervision. ICC is the generalisation of urban applications OCC of all types of railway supervision. Newest networks as high-speed line in France use an ICC called train-regulating signal box that deliver both level one and two of high-speed line. The third level cannot be integrated in such circumstance because of the existence of few connections with other national switching zone (as specific signal boxes for large stations managements for example). Indeed,

management and planning must be decided in a highest regional or national commandment.

At the same time, Automatic Train Control system (ATC) performs three underlying functions in railway application: protection, driving assistance and supervision. In this system, supervision function is performed at the ICC and the train driver's tasks could be simplified considerably and safety stems from protection.

Figure 4: Photography of ICC.

3.2 Automatic Train Control

ATC system is composed of three subsystems giving in decreasing order of underlying safety: Automatic Train Protection, Automatic Train Operation and Automatic Train Supervision. The followings sections present each subsystem.

3.2.1 Automatic Train Protection

Automatic Train Protection system performs a range of functions that protect passengers and equipments against principal dangers related to railway circulation (collisions between trains, collisions with objects, excessive speed, derailments). The line is cut out in sectors called blocks or track sections. Spacing between trains is ensured by the function of block occupancy management. Train detection by track circuits (one track circuit per block) indicates train position and insures trains spacing. The guiding principle of railway safety consists, via side signals indications, to authorize the presence of only one train by section. In the majority of cases, sections are fixed (fixed block) and side signalling consists of traffic lights in limits of each block. For the most recent systems, blocks are moving with the train and their length are evolving with train's speed and way occupation (moving block), which allows an optimization of line's transport capacity. In both cases system ATP is able to detect incompatible speeds in accordance to stop limit distances at the end of sections and at extreme the penetration on occupied sections (and naturally acts as consequence by an emergency braking of the train if one of these events occurs). The usual terminology distinguishes from the ATP the interlocking whose essential function is to prevent incompatible movements of trains on the switching zones.

3.2.2 Automatic Train Operation

Automatic Train Operation or "autopilot" controls fully or partially the trains according to a fixed timetable. Timetables are defined each day to prepare and organize exploitation. ATO manages programmed stops in stations, doors control and the dwell time respect. Then it starts again the train after each stop in case of integral automated system. In partial automation cases, doors opening, doors closure and depart order are given by aboard operator (driver or "attendant").

3.2.3 Automatic Train Supervision

Automatic Train Supervision insures monitoring of all subsystems which compose the line (trains included) and regulation functions. Each components state are represented on visualisation panels called Schematic Control Panel (SCP) presenting a global view of the line and on the working stations of operators which can provide more or less detailed sights and tables or graphs of telemetries. Information presented can thus be more or less fine according to operational constraints' of the line. The ATS thus makes it possible to apprehend in a total way the state of line operation (by the synoptic in general presented at SCP which presents in real time information as sections occupied, switching points position, energy state, etc.). It can also focus operator attention on particular equipment (fixed or on board a train) via telemetries also updated in real time, allowing alarms visualisation on which operators can obtain details. The ATS also presents data making it possible to ICC operators to carry out traffic flow control (for intercity networks, this function is carried out by a particular operator called regulator) which consists to decide the appropriate actions in case of incident to restore a (possibly degraded) mode of operation. Depending of the detail of the situation, other trains on the line could be delayed in order to manage intervals.

3.3 Safety

CENELEC is a safety reference frame. It is particularly applicable to railway domain and is composed of the following standards: EN 50126 [5], EN 50128 [6] and EN 50129 [7]. With this reference frame, the safety measure can take a value among five possible. The smallest SIL (Safety Integrated Level) is 0 when the evaluated application is not critical. The highest SIL is 4 when the evaluated application is very critical. For example, an application is SIL 4 when many human lives are concerned.

As we explained, safety is ensured by the ATP (Automatic Train Protection) functions and interlocking. At the beginning, all these features were implemented with safety relays and analogical circuits. These implementations use *intrinsic fail safe design* (no single failure or likely combination of failures can lead the system to a less safe state than that before the failure). Since several years, numerical systems are emerged in ICC implementation. These systems are SIL 3-4. Thus, the development of such systems needs rigorous methods like those presented in the safety reference CENELEC. These methods concern as much hardware devices as software ones. Finally, numerical systems have several advantages. They are flexible and they have a smaller size than relays

and analogical circuits. For these reasons, ATP and interlocking implementation with numerical solutions will be generalized in the future.

ATO (Automatic Train Operation) features are built on a complex system control. The main consequence is that SIL 3-4 insurance is not reached for this system. Nevertheless, when ATO failures occur, the ATP is charged to catch up the problem. For example, ATO can emit an order that cause an inopportune acceleration. In this case, as ATP controls safely the speed, it can cause the stopping of the train by emergency braking. Thus, ATC safety approach is built on ATO, which safety designed.

Similarly, ATS is not considered classically as safety critical like ATO. In addition, the ATS conception is based on COTS (Commercial Off the Shelf) components. The main objective is to reduce the manufacturing costs. But, the SIL level of COTS components is practically not established. Moreover, the safety analysis of COTS components is practically impossible because the required data are not provided. Nevertheless, several accidents and incidents analysis clearly showed that although the origin of a safety problem could never be attributed to the ATS, an adapted management of a crisis situation and an adequate decision of a quite well informed supervision operator could seriously reduce accidental scenarios consequences. More precisely ATS features assist the operator to execute procedures adapted to the different scenarios an exploitation mode. And, an important report has been done: more the exploitation mode is degraded, more the ATS role is important to ensure safety.

The present context, underlaid by a legitimate concern for the profitability of the infrastructures, considering the competition of road transport (either transport of passengers or transport of freight), generally leads to operating the lines up to their maximum capacity (at least during certain time slots), which thus provokes a strained flow management, requiring, when an operator's intervention is needed, very short delays. Additionally, the human operator getting used to the automation of some tasks which were his in a recent past, is very little trained to act when those helps are not available to him, cases that are precisely situations of crisis. The result of this is at best a clearly enlarged period before the appropriate reaction, effect which adds itself to the growth of traffic mentioned above. In the worst cases, given that the instructions do not usually consider thoroughly the scenarios in which the information about the state of the system is unavailable or very damaged, some completely inappropriate actions from the human operator can be observed (so as to make the situation even worse). The analysis of such scenarios often shows that the operator, for lack of complete and reliable information about the state of the system, creates for himself a coherent but erroneous mental outline in great hurry, on which his decisions will be based; the tension linked to the crisis making him carrying on regardless of other possible plans compatible with the information available to him.

For all the reasons mentioned above, the possible impact of supervision system on safety must be studied, as much for applications of urban transport as of main lines passengers and freight transport (the last two moreover usually sharing the same infrastructures).

4 SPICA rail platform

Studies on human operator behaviours experiments will be performed at the University of Technology of Compiègne (UTC) using a supervision platform "SPICA-Rail" similar to a real one (Alstom Transport's supervision product: ICONIS™), installed in our research center (see photography Figure 5:). This equipment will of course include an "environment simulator" making it possible to do "as if" the experimental platform would be really connected to a railway network. The main interest will be the possibility to re-create in laboratory real accidental scenarios, and to be able to confront human operators with these situations, in order to analyze their comportment and their decisions.

Figure 5: Photography of SPICA rail platform.

This platform is already installed but still in validation process. Such experiments suppose a clear definition of requirements to define the most adapted railway network to analyze contribution of supervision's process in safety. ICONIS™ product is a generic product of railway supervision based on SCADA. For each project, an instance is defined from generic modules of ICONIS™ and datas defining project properties as for example: track plan, stations, switching points or signalization rules. The ATS system installed in UTC includes three levels of control on traffic: manual automated and optimized. The network simulated is divided into interlocking zones (or switching zone). Each zone disposes of local ATS system where operator could take control supervision locally. The global supervision is centralized in a central ATS which gather all local ATS information and command.

SPICA-Rail could simulate the control and the supervision of an entire network by integrating traffic control functions. It includes a wide range of traffic control and management functions including for example: signalling supervision, route setting, train tracking, train describer and timetable management.

In order to simulate crises situation, personal subject of experiment behaviour will start from an automatic control level in which all operations have an

objective to comply with an operational schedule (timetable) and network regulation. Experiments consist with increasingly insert disturbance on the network and evaluate human behaviours.

5 Conclusion

Safety development of supervisory software is far from obvious, but we argue that well-understood interfaces between man and machine could contribute in safety. Major problem come from bad requirements. Our purpose intends to analyse human supervisor behaviour in such particular serious cases in order to highlight lack in requirements. Capability for safety and automate working adequacy of human performance are the underlying research plan.

As a conclusion we expect to propose a methodology to develop new supervision systems taking into account human factor from the beginning of the design process. That will make it possible to use a process by *feed forward* (anticipation based on preliminary studies [2]) instead of a process by *feedback*.

References

[1] Sheridan, T. B., *Telerobotics, Automation, And Human Supervisory Control*, Cambridge, MA:MIT Press, 1992.
[2] Norman, D.A., *The invisible computer: Why good products can fail, the personal computer is so complex, and information appliances are the solution*, Cambridge MA: The MIT Press,. 1998.
[3] Boyer, S.A. SCADA: *Supervisory Control and Data Acquisition*, ISA-The Instrumentation, Systems, and Automation Society, 2004.
[4] Ramadge P. J., Wonham W. M., Supervisory control of a class of discrete event process, *SIAM Journal on Control and Optimization*, **25(1)**, pp. 206-230, 1987.
[5] CENELEC EN 50126: Applications ferroviaires – Spécification et démonstration de Fiabilité, Disponibilité, Maintenabilité et Sécurité (FMDS), 1999.
[6] CENELEC EN 50128: Applications ferroviaires – Système de signalisation, de télécommunication et de traitement – Logiciels pour systèmes de commande et de protection ferroviaire, (2001).
[7] CENELEC EN 50129: Applications ferroviaires – Système de signalisation, de télécommunication et de traitements – Systèmes électroniques relatifs à la sécurité pour la signalisation, (2001).
[8] *Webster's Encyclopaedic Unabridged Dictionary of the English Language,* Grammery Books.