TECHNICAL PRESENTATION OF ATO OVER ETCS SUSING THE SUBSET 125 FOR FREIGH TRAINS

SIMON COLLART-DUTILLEUL[1] , PHILIPPE BON[1], RACEM BOUGACHA[1] & RÉGINE LALEAU[2]
[1]Univ. Eiffel, COSYS/ESTAS, Villeneuve d'Ascq, France
[2]Université Paris-Est Créteil, LACL, Créteil, France

ABSTRACT
This presentation decribes the context a the freigh train use case concerning ATO over ETCS for a grade of Automation level 2. It mainly focus on the specification and does not focus on system analysis consequences of the design architecture as in [1]
Keywords: Model engineering, Formal method, ERTMS, Automatic Train Operation (ATO), AoE, Grade of Automation (GoA), Autonomous freight Train

1 INTRODUCTION

Checking the closed door is not as critical for a freight train as for a passenger train and some generic requirements are not considered in the implementation of Subset 125[2]. Nevertheless, in both cases, the beginning of a train mission mostly starts with a phase where a human has to manage with the situation's uncertainty until it reaches an ERTMS beacon. At this point, its position is perfectly known and the train can receive a Movement Authority (MA) and use a Full Supervision (FS) mode. Under this particular functioning, the behavior of the driver is supervised. It means that, in case of over-speed, a warning is triggered, then service brakes, then emergency brakes. As a consequence, they are several kinds of phases in a train mission. In some of them, the main conditions of a safe functioning can be automatically checked and maintained, in other ones, a human actor is needed. In order to perform an industrial implementation of the above concepts, automatic and non automatic phases must be clearly identified. A preliminary condition seems to be the definition of a normative framework. Moreover, a methodology ensuring the rigorous implementation of this framework is an important contribution to its industrial efficiency. The current section proposes a system analysis on the basis of normative and pre-normative documents. Corresponding UNISIG Subsets will be mentioned all along the current document to explain how an Automatic Operation System (ATO) can be supervised by ETCS. Then a main high-level requirements model for automatic train operation is presented and the architecture of AoE on the basis on available normative or pre-normative documents is detailed. Finally, a SysML model of the described architecture is introduced as a starting point for an automated software generation.

1.1 Drivers of GoA2 systems

There are several Grades of Automation (GoA) for trains. The highest one, Level 4, does not require any human contribution for driving trains and is called GoA4. The French VAL system (Véhicule Automatique Léger) which is operating on the Lille Metro since 1983, is a fully automated GoA4 system. A similar ATO system is also used with conventional rolling stock on the Paris Metro Line 14 and Line 1. The Swiss Lausanne Metro line 2 uses the same system. Readers interested by more information concerning relationships between GOA2 and GOA4 may consult [3].

Considering a freight train running with a GoA2 system, a human driver drives the train "when needed" and handles emergencies. "When needed", may corresponds to particular operational test cases. A wide list of classical emergency cases can be found in Section F of RCL [4]. RCL is more than 1300 pages document describing principles for a French driver behavior. It is used and periodically updated by teachers in learning centers. It is assessed by various railway experts. To give an example, in Section F of RCL, the procedure "obstacle protection" is documented. It details what to do when a rock or a fallen tree is laying on railway tracks. In case of GoA2 functioning, the driver identifies the problem and switches off the ATO. Then, he applies the specific procedure. In case of GoA4 functioning, new procedures have to be introduced as there are no driver able to apply the existing procedure. In terms of requirements, it means that the driver should be able to take the control of the train efficiently while it was running automatically. In the case of a pure GoA2 functioning, the driver is mainly in charge of his own awareness. In other words, he is supposed to supervise the automatic driving in such a way that he is fully able to operate when it is needed. To give an example, in case of an emergency braking, the driver is supposed to know if the emergency brake is not occurring because of the train has passed through a red light, but for another reason. An information missing can lead to a wrong evaluation of the current situation, and then to a wrong decision. Let us introduce a deeper illustration about awareness. Let us suppose a car driver drives using a function of his car known as "autopilot", corresponding to GoA2. When the driver takes back control in order to manage a situation of emergency:

- he is supposed to know whether there is a vehicle just behind his car;
- he is supposed to be aware of the presence of an emergency stopping lane adjacent to the road;
- he is supposed to know if he is driving on a high-way or on a two-way traffic road.

These three pieces of information are instances of data, which have to be available, because they are needed to take an emergency decision for obstacle avoidance. For all these reasons, a GoA2 car driver is regularly required to put his hands on the steering wheel of the car. This is expected to be a sufficient measure to ensure the driver's attention. There are two classes of emergency scenarios:

- when the automatic driving GoA2 system identifies that it is not able to manage the current situation;
- when it identifies no problem, but an outside monitoring loop diagnoses the need of an emergency management.

The first case corresponds to an obstacle detection, which a GoA2 train driving system may know that it is not able to handle: in the current existing procedure, a human has to put warning devices on the tracks in order to prevent another train to collide the obstacle. The second case may correspond to the vision of a ball crossing the railway track, at five o'clock in the neighbourhood of a school building. The GoA2 system may identify the ball as a non-dangerous entity when it has the sensors and associated software able to do so, because a collision with a ball does not damage the train at all. Moreover, if the ball is damaged, its commercial value can be neglected. Nevertheless, an experimented driver may know that a ball in the neighbourhood of a school, at this moment of the day and in the current range of date is linked to a high probability of children running after the balloon. In the considered use cases, information of the GoA2 system needed for the emergency management performed by the driver must be provided: it seems to lead to specific ergonomic requirements, as the the format of the information needs to be adapted to the particular mission that the driver is performing. These requirements are not considered in the current paper, only identifying the main entities and their nominal relations.

1.2 ATO GoA2 running over ETCS

When an ATO is running over ERTMS, there is no influence on the global goals. ERTMS can be seen as an implementation constraint which makes things simpler, as the functional specification of a rolling stock behavior is provided in Subset 26 [5]. The concerned component is called EVC (European Vital Computer) and its communication with peripheral components is specified too. The interface specification defines the functional interface between the ERTMS/ETCS on-board equipment and the vehicle [6]. On the web site of the European commission, one can read: “The railway interoperability Directive 2016/797 of 11th may 2016 [7] sets out the conditions to be met to achieve interoperability within the Union rail system”. Interoperability is a way of providing better performance of the global European railway system, and it is a means to provide safety while managing the diversity of European railway infrastructures and European rolling stocks.

1.2.1 ERTMS system

ATO operates under ETCS supervision and does not affect safety [8]. The basic principle for ensuring safety while providing interoperability embedded into the ERTMS architecture is to split responsibilities between operational stakeholders.

- Trackside system (under the responsibility of the infrastructure manager) sends track description, which content has to be semantically aligned with “ETCS language” and ETCS rules.
- ETCS on-board systems implement ETCS-specified behavior, according to messages received from the trackside system.

1.2.2 ATO over ETCS (AoE)

The track, i.e. the global system management of the infrastructure holder, provides two different sets of data being specified respectively in Subset 131 [UNI131] and in Subset 132 [UNI132] . The global architecture of the system (see Figure 1) in a nominal functioning can be seen as a three layered one.

On the top, there is the ETCS supervision. Particularly in Full Supervision (FS) mode, the ETCS OB system may apply a “service braking” in case of small over-speed. In case of heavy over-speed, the ETCS OB system will trigger an emergency braking, triggering the TRIP mode. At a second level, the driver sends a message to get in Automatic Driving mode, by the means of the Display Machine Interface (DMI): the DMI is the normalized human interface using ERTMS. This message asks to trigger the process towards ATO mode. As detailed in [9], Subset 126 details the ATO OB (On-Board) - Vehicle Interface, allowing the ATO OB to control the vehicle. AoE specifies the interface between the ATO on board and the physical vehicle in Subset 139. ATO OB - ETCS OB Interface defines the needed data and the corresponding operational protocol allowing exchanges between a software entity running in the automatic train and the hardware and software entities corresponding to the ETCS technical specification. It is detailed in Subset 130.

This Interface includes:

- ATO Status (”AD Mode request”, ”ATO Engaged”)
- ETCS Train Data (e.g. ”Train length”, ”Maximum Train Speed”, ”operational train running number”)
- Dynamic ETCS Data (e.g. ”Positioning Information”, ”MA Information”, ”Speed Information”)

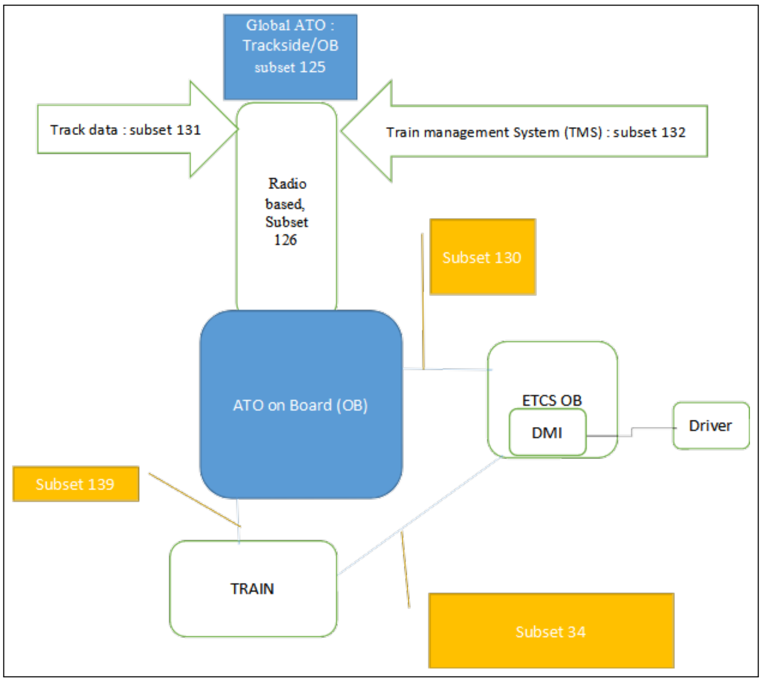


Figure 1: Extract of the architecture of ATO over ETCS

As an example, ATO OB needs to receive train data, which are provided by the driver running the ERTMS/ETCS procedure called “data entry”. Among other information, a data entry provides the length and the nature of the train. Obviously, this information is needed to smartly control the train. In the context of a GoA2 functioning, the driver may send the following orders to ATO OB through the human interface of ETCS OB called DMI:

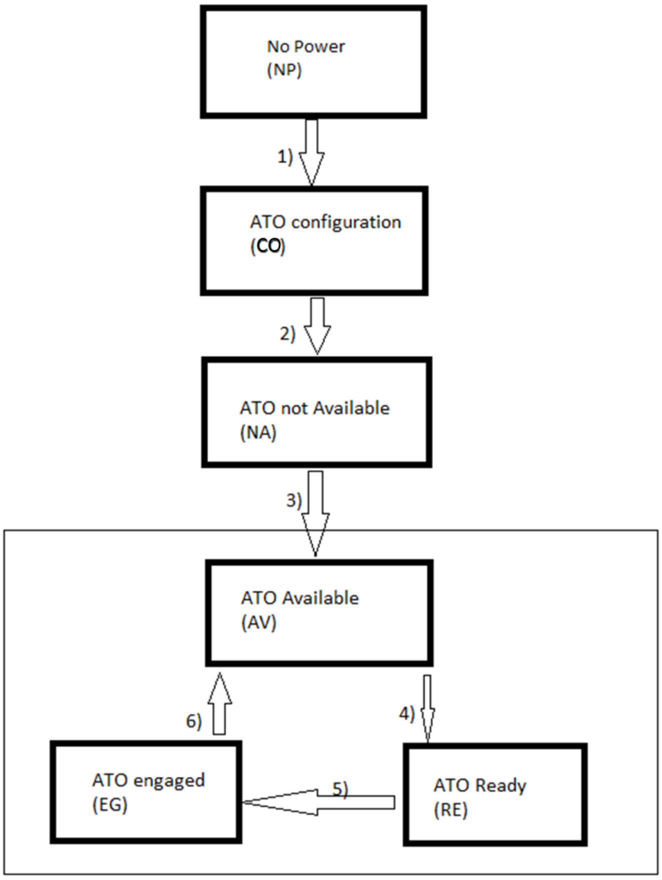
- ATO Engage: Used by the driver to request the start of automatic driving (departure of the train or engagement on the move).
- ATO Disengage: Used by the driver to disengage ATO while the ATO OB is engaged.

The “ATO Disengage” input is considered as enabled by the ETCS OB when the ”ATO engaged” or when the “ATO Disengaging” indication is displayed. Some national signalling systems may benefit from the normalization of interfaces between trackside and on-board systems [2, 10, 11, 12, 13]. The table in Figure 2 may be consulted for more information on the ATO mode state management.

1.2.3 Functional analysis conclusion

What are the advantages of using Subsets 131 and 132 under AoE, using a GoA2 autopilot ?

1. The computer is more efficient at processing dynamic information in real time without making any error.
2. The driver is in charge of other safety goals, he is therefore not supposed to make heavy calculations in real time which may create loss of attention. Functions such as ”monitoring the environment” are clearly specified in the ”RCL” as being the driver’s tasks [4]. The work-load of a driver adapting his driving strategy to a continuously



1)	The ATO-OB is powered on. The ATO state changes from NP to CO. The "**ATO Selected**" indication is displayed
2)	ETCS data entry process (including ATO Specific Data Entry) is completed and the ATO-OB receives the required data. The ATO state changes from CO to NA. The "**ATO Selected**" indication is displayed.
3)	When all the ETCS related Conditions are fulfilled and ATO global infrastructure is detected, the ATO state changes from NA to AV and the "**ATO Available**" indication is displayed to the driver.
4)	When all the ATO Engagement Conditions are fulfilled, the ATO state changes from AV to RE and the "**ATO Ready for Engagement**" indication is displayed to the driver.
5)	The driver selects "**ATO Engage**", the ETCS changes to AD Mode. The ATO state changes from RE to EG. The "**ATO Engaged**" indication is displayed to the driver and the ATO-OB starts driving the train automatically
6)	The ATO-OB drives the train. When the train stops, the ATO-OB requests the "**Train Holding Brake**" application and the "ATO Selected" indication is again displayed to the driver. The state changes from EG to AV. The train is stationary waiting until the ATO Engagement Conditions are fulfilled again.
7)	Return to step 4) and repeat the sequence until the end of the journey

Figure 2: ATO states for a nominal scenario, out of draft of Subset 125.

changing environment including timetables real time adaptation with regards to delays of ongoing missions of other trains, may decrease his ability for checking the safety of his mission.

As such, it is the driver who guarantees that the context of the GoA2 operation ("No safety function other than compliance with signs") is fulfilled by the ATO. When the ATO is running, the work-load of the driver is decreased in such a way that his level of awareness of environmental evolution may increase.

REFERENCES

[1] Collart-Dutilleul, S., Pereira, D.I.d.A. & Bon, P., *Designing Operating Rules for ERTMS Transnational Lines*, Springer International Publishing: Cham, pp. 133–161, 2022.

[2] Subset-125: ATO over ETCS – system requirements specification. (issue: 0.1.0). Std, UNISIG, 2018.

[3] ATO over ETCS: A system analysis for freight trains. *WIT Transaction on The Built Environment, COMPRAIL 2022, Valencia, Spain, 21-23 September, Proceedings*, eds. G. Passerini & J. Mera, WITpress, volume 213, pp. 37–47, 2022.

[4] SNCF specific driver rulebook for operating train in France, *Référentiel conducteur de ligne*.

[5] Subset 26: "system requirements specification". Std, UNISIG, 2016. Https://www.era.europa.eu/content/set-specifications-3-etcs-b3-r2-gsm-r-b1_en.

[6] Subset 119: Train interface FFFIS. Std, UNISIG, 2020. Https://www.era.europa.eu/content/informative-set-specifications-3-etcs-b3-r2-gsm-r-b1_en.

[7] European Commission, Directive 2008/57/EC on the interoperability of the rail system within the european union. Technical report, European Union, 2016. Https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0797&qid=1680166548159&from=EN.

[8] Bienfait, B., ATO over ETCS, 2016. Https://slideplayer.com/slide/14324166.

[9] Kuhn, M., System architecture description, smartrail 4.0 architecture. Technical report, Smartrail 4.0, 2019.

[10] Subset-126: ATO over ETCS – ATO-OB/ATO-TS FFFIS application layer specification. (issue: 0.0.16). Std, UNISIG, 2018.

[11] Subset-130: ATO over ETCS – ATO-OB/ETCS-OB FFIS application layer. (issue: 0.1.0). Std, UNISIG, 2018.

[12] Subset-139: ATO over ETCS – ATO-OB/ vehicle interface specification FIS. (issue: 0.0.8). Std, UNISIG, 2018.

[13] Buurmans, K., Automatic train operation over legacy automatic train protection systems, a case study on the groningen-buitenpost line. Technical report, Delft University of Technology, 2019. Master of science in civil engineering at the faculty of Civil Engineering and Geosciences, department Transport & Planning of Delft University of Technology, https://repository.tudelft.nl/islandora/object/uuid:dffc21d9-936c-4286-9611-a2a846cfc416?collection=education.