ATO OVER ETCS: A SYSTEM ANALYSIS
FOR FREIGHT TRAINS

PHILIPPE BON¹, SIMON COLLART-DUTILLEUL¹ & RACEM BOUGACHA²

¹Univ. Eiffel, COSYS/ESTAS, France
²Institut de Recherche Technologique Railenium, France

ABSTRACT
Automatic train operation under the supervision of a human driver is sometimes presented as a first step toward autonomous trains. This paper provides a system analysis of the available norms dealing with automatic train operation under driver supervision. Clarifications that have to be introduced to make it compatible with an autonomous train module are highlighted. Then, the work focuses on the collaboration between an automatic software for braking and accelerating in the European normative and technological context, known as ATO over ETCS. The study of the available documents allows proposing an architectural model of this global system containing on board automation and on track automated specific devices. The main motivation behind using this technical architecture is to trace a future implementation that preserves the high-level goals. This technical contribution is a first step for building an integrated approach to specify a correct system by construction, conforming to the industrial norms of automated train. In this paper, we explain how it is relevant to use a norm based technical architecture, providing intellectual references that allows drivers to identify various functioning phases where, depending on the overall context, they can let an automatic system drive the train or not.

Keywords: ERTMS, automatic train operation (ATO), ATOoETCS, 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. 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” mode (FS). Under this particular functioning, the behaviour of the driver is supervised. It means that a warning, then service brakes, then emergency brakes will be triggered. As a consequence, they are several kind 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 presented paper proposes a system analysis of a functioning which is automated in some phases and driven by a human in other phases on the basis of 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. The second section presents main high level requirements for automatic train operation. the third section details the architecture of ATO over ETCS on the basis on available normative or pre-normative documents. In a fourth part of the paper, a SysML model of the described architecture is introduced as a starting point for an automated software generation, this model being by construction conform to the modelled normative framework.
2 TECHNICAL MOTIVATION FOR AN ATO SYSTEM

There are several Grades of Automation (GoA) for trains. The highest one, the 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 too.

2.1 GoA2 and GoA4

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 the Section F of the RCL [1]. The RCL is a more than 1300 pages document describing principles for a French driver behaviour. It is used and periodically updated by teachers in learning centres. It is assessed by various railway experts. To give an example, in Section F of the RCL, the procedure “obstacle protection” is documented. It details what to do when a rock or a fallen tree is laying on the railway tracks. In case of GoA2 functioning, the driver identifies the problem and switch 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 its own awareness. In other words, he is supposed to supervise the automatic driving such a way that he is fully able to operate when it is needed. To give an example, in a 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 its 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 piece 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.

When the emergency management is provided by a software entity, the situation has to be analysed deeper. 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 knows that it is not able to handle: in the current existing procedure, a real 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 case, the emergency management need is identified using a knowledge, which is not embedded in a common GoA2 driving system.

To conclude this section, authors want to highlight that the definition of a GoA2 automation system being compatible with GoA4 is difficult to establish, because it is not standalone. It depends clearly on the GoA4 monitoring services that are running in parallel in order to diagnose difficult scenarios. When the monitoring GoA4 layer does not build its own knowledge on history, the GoA2 system has to share its needed variable states in order to complement the knowledge of the GoA4 system. Today the state variables needed for the management of a GoA4 train system are not formally defined in the literature. Therefore, complementing this undefined set of variable cannot be formally achieved, on the basis on normative or pre-normative documents that we have consulted. Nevertheless, this is a work to perform, before being able to specify a GoA2 system “compatible with GoA4.” It would be a step forward towards the autonomous train.

2.2 GoA2 train

In the literature of requirement engineering, “goals are desired system properties that have been expressed by some stakeholders” [2]. The main motivation of their usage in requirement engineering is justifying requirements by linking them to higher-level goals. A railway system has to be safe. As a consequence, the first high-level goal named G1 is needed to receive an authorisation of commercial exploitation from the National Safety Agency.

- **G1: “The system should be safe.”**

In the subset 125 normative document proposing a GoA2 framework [3], the driver is in charge of managing safety related events, whereas the autopilot software deals with non-critical situations.

From the previous analysis, it is proposed to specify a GoA2 services, potentially compatible with a GoA4 system on a main line. The goal G2 and G3 can be expressed as follow:

- **G2: The GoA2 system should respect signals and speed limits. When it is not able to do so, it should formally specify its situation.**
- **G3: The GoA2 system should take into account timetables and condition of traffic in order to respect the timetables of the global system.**

Analysing G2, respecting signals and speed limit is a necessary safety condition. Nevertheless, in case of default of the braking system, it may happen that a common braking distance cannot be applied [4]. In this case, values of last signals and last braking distances associated to well defined control orders should be communicated. The best contribution of the GoA2 system is to share its knowledge. In other words, values of the variables allowing to identify that the limit of the GoA2 functioning has been over-passed should be accessible for the GoA4 system. Moreover, the semantic of the considered state variable has to be
formally defined. Let us recall to mind that a common ontology of all actors of the railway system, named Ontorail (https://ontorail.org/wiki/), has been introduced by the International Union of Railway (UIC). Nevertheless, concept definition is not sufficient for scenario identification. In order to characterize a given situation in a professional railway context, the RailTopoModel (http://www.railtopomodel.org/en/) standard may be used. Finally, when a precise and rigorous description is needed, the dynamic scenario can be specified by the mean of Goro [5]. Examples of using ontology engineering in order to model railway accidents can be found in the state of the art [6]. All these considerations lead to claim that state variables leading a GoA2 system to the self-characterization of its own limits of functioning should be formally defined, as they can technically be formally defined.

The following of the document focuses on the specification of a GoA2 services, potentially compatible with GoA4 of a freight train while running ERTMS.

3 ATO GOA2 POTENTIALLY COMPATIBLE WITH A GOA4?
The fact that the implementation of an ATO is implementing ERTMS does not have any influence on the global goals. ERTMS can be seen as an implementation constraint. This implementation constraint makes things simpler, as the functional specification of a rolling stock behaviour is provided in the subset 26 [7]. The component in question is called EVC (European Vital Computer) and its communication with peripheral components is specified too. The interface specification defines the form fit functional interface between the ERTMS/ETCS on-board equipment and the vehicle [8]. On the web site of the European Commission, we can read: “The railway interoperability Directive 2008/57/EC of 17 June 2008 [9] 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 infrastructure and European rolling stocks.

3.1 ERTMS System

ATO operates under ETCS supervision and does not affect safety [10]. The basic principle for insuring safety while providing interoperability embedded into the ERTMS architecture is to split responsibilities between operation 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 behaviour, according to messages received from the trackside system.

3.2 ATO Over ETCS (ATOoE)

In order to fulfil high-level goals G2 and G3, the track, i.e. the global system management of the infrastructure holder, provides two different set of data being specified respectively in subset 131 [UNI131] and in Subset 132 [UNI132] as presented in the final conference presentation of X2Rail-1 (https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1, slides 16 and 17). The global architecture of the system (see Fig. 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
Figure 1: ATO over ETCS, partial architecture.

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 [11], the Subset 126 details The ATO OB (On-Board) – Vehicle Interface, allowing the ATO OB to control the vehicle. ATO over ETCS specifies the interface between the ATO on board and and the physical vehicle in the 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 detail in the 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., “EB is requested,” “Positioning Information,” “MA Information,” “Speed Information”).

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
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 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.

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.
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 system may benefit from the normalization of interfaces between trackside and on-board systems [3], [12]–[15]. The table presented on the Fig. 2 may be consulted for more information on the ATO mode state management.

3.3 Functional analysis conclusion

What are the advantages of using subset 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” line repository as being the driver’s tasks. The work-load of a driver adapting his driving strategy to a continuously changing environment including timetables real time adaptation with regards to delays of ongoing missions of other trains, decreases 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. When the ATO is running, the work-load of the driver is decreased in such a way that his level of awareness of environmental evolutions may increase.

4 ATO OVER ETCS SYSTEM ARCHITECTURE

As presented in the previous section, when the system switches from a human driver to an automatic system, abilities of the driving agent change. A consequence is that configuration changes on the track-side and on the on-board system, using the communication means provided by the subset 126.

The current section provides a global description of the corresponding architecture using SysML block-diagrams [16]. It is detailed by presenting state machines of each of the 3 first layers. The last layer and sequence diagrams are not presented in the current paper. To model the GoA2 ATO over ETCS System architecture, the system is broken down into 4 levels (see Fig. 3).

The first one (see Fig. 4) “ATOoETCS_GOA2SystemL0” represents the abstract system, that contains only one element named “ATOoETCS_GOA2SystemL1.”

The second one (see Fig. 5) “ATOoETCS_GOA2SystemL1” represents a refinement of the Level 0. It introduces two components, Track and On board, as specified in subset 125 [3] and can be seen in the blue components of Fig. 1.

In the level 2 there are 2 subsystems “Track” and “OnBoard” as components of “ATOoETCS_GOA2System” element of level 0. The third level (see Figs 6 and 7) is a
decomposition of the second level into five components. Track is decomposed into (ATO-Track, RBC) and Onboard is decomposed into (ATO-Onboard, ETCS and Train). One can notice that in the two first levels, a logical architecture able to manage the various functioning phases is presented. This specification concerns mainly software and automation. At this level, the mechanical part of the system appears with the component train. Messages exchanged between components of Onboard are normalized respectively by subsets 130, 34 and 139 as shown in the lower part of Fig. 1. This specification can be integrated in the port definitions of corresponding Block definition Diagrams modelling the on board system description at level 2.

In the last level, ETCS is decomposed into (ATP, DMI, DRIVER), which are not presented here. We have to notice that the driver may not be a component of the system, because in a Jacobson schema he would be an agent triggering functions by the mean of the DMI. A more relevant analysis consider the driver to be a component of a GoA2 system (see Fig. 1). Adopting this point of view, the human is not only an agent triggering functions; he is one of the components of the global system (see Fig. 3). As a consequence, his operational ability has to be ensured by the system. It means that interactions with the autopilot induce a sufficient
Figure 5: Level 1.

Figure 6: Track at Level 2.
level of attention and a coherent understanding of the operating context. By adopting this point of view for the ATO GoA2 system analysis, a high level goal, in the sense of Kaos methodology [2] is elicited. In this methodology, goals are expressed by requirements. As an example, periodic task has to be allocated to drivers in order to maintain their attention and the system has to provide to drivers necessary information for transient mode handling. Consequently, this goal produces specific proof obligation injections in the event-B model that insures a fully compliant implementation with regard to this high level need.

5 CONCLUSION AND FUTURE WORKS
The paper presented a system analysis of a pre-normalized technical solution for ATO GoA2 functioning. It consists of using an automatic operation system over ETCS, while a driver is in charge of safety relevant operations. Analysing normative or pre-normative documents, assumptions of functioning are explained in a first part of the paper. In a second part, a SysML model of the higher levels of the architecture is provided. This is a first step of an approach which is “correct by construction”. Using a Kaos methodology [2], some event B abstract machines [17] may be generated from the SysML architecture, where some invariants modelling the main goals of the architecture can be proved. Thorough the whole paper, some high level goals were presented. Moreover, going out of an ATO supervised functioning is not a simple shift from a functioning to another and the awareness of the driver – this driver can be a human or a intelligent GoA4 software – is a problem to be considered. Focusing on this technical challenge, new specific goals (in the sense of the KAOS approach) have to be introduced. These Goals are to be translated in Event B invariant insuring that the initial need are tracked toward a safe ATO software implementation. Clearly, further works concerning model engineering still need to be undertaken.

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


