Decentralized-Hierarchical Control Approach Automatic Train Protection (ATP) of Communication Based Train Control (CBTC)

Cem Atilgan, Özgür Turay Kaymakçi, Tarik Veli Mumcu

Decentralized-Hierarchical Control Approach Automatic Train Protection (ATP) of Communication Based Train Control (CBTC)

Cem Atılgan[1], Özgür Turay Kaymakçı[2] ,Tarık Veli Mumcu[3]

Abstract

As the number of people living in metropolises are increasing with urbanization, the demand for metro systems, which are accepted as the main mode of modern urban transportation, is increasing especially in big metropolises such as Istanbul. As a result of this change, a higher performance is expected from Communication Based Train Control (CBTC) systems today, such that the reduction of the headway without compromising reliability and safety will be one of the primary goals in the coming years. From wireless communication infrastructure to vehicle dynamics, so many factors appear in the improvement of this challenging problem. On the other hand, some subsystems of CBTC such as Automatic Train Protection (ATP) are expected to implement the desired safety functions with the highest level of safety without being affected by these evolving technologies and increasing requirements. However, the generic design of these systems may need to be modified according to these new requirements. In this context, formal modeling methods and the development of supervisory controllers within these context are of great importance.

In this study, CBTC and its subsystem ATP are modeled by finite state automata with discrete event system approach. It has been shown that the corresponding supervisory controllers meet the controllability and non-locking control conditions. Furthermore, the results are compared with the monolithic approach structure.

Keywords Finite State Automata, Decentralized-Hierarchical Control, Communication based Train Control, Automatic Train Control, Automatic Train Supervision, Discrete Event System

1 Introduction

Today, the most important infrastructure of train and metro systems are signaling systems. Signaling systems allow trains to move safely on the rail line while regulating train traffic. In parallel with the development of today's technology, the infrastructure of the signaling systems is developing day by day. Many countries within Europe are working on various signaling systems projects equipped with the latest technological infrastructures. European Rail Traffic Management System (ERTMS), which will serve to make rail transport safer and more competitive, is a major industrial project being implemented by Europe [1]. On the other hand, Swiss Federal Railways (SBB) and Scheidt & Bachmann System Technik GmbH (CSC) jointly developed the dispatching level of the Rail Control Systems (RCS)[2]. Some of the studies on signaling systems are as follows: MOVINGRAIL the project will bring innovative concepts of moving-block railway traffic operations by advance testing methods for European Train Control Systems Level 3 and virtual coupling analysis, which will lead to convoys of automated trains under cooperative adaptive control. Another project in signaling systems is X2RAIL. X2RAIL-1, X2RAIL-2, X2RAIL-3 and X2RAIL-4, these projects include advanced signaling and automation systems. The aim of these projects to enhance traffic management system functions as well as increase capacity, autonomy, and flexible communication. ASTRAIL enhanced version

of the ERTMS with Moving Block Systems, Automatic Train Operations (ATO) and global navigation satellite systems positioning provide a palpable improvement in the quality of the European railway transport system, while providing a solution to the problem of increasing requisition on high-density lines[3].

Communication-based train control (CBTC) is one of the safety-critical application systems in the railway. With the rise of the complexity of the system, proper development method is required during the CBTC software system development life-cycle. Functional and safety necessities play a vital role. The internal structures of the sub-systems such as Automatic Train Supervision (ATS), ATO, Automatic Train Protection (ATP),etc. within CBTC, that consist of critical systems such as signalization used in the mentioned projects are complex. It is very essential to control these complex systems for the safety and the interoperability of the trains and other systems. The structure of the system is required to be modeled to minimize the complexity of these structures. Modeling the form brings the following edges to the system: it facilitates the traceability of the system, It simplifies the design of the controllers, the last but not least in case of an error, it provides shorter intervention time to the system.

When CBTC is desired to be modeled with finite state automats, the excessive number of subsystems it contains causes the state space explosion. In such a situation, the supervisory controller synthesis becomes very difficult and the computation time becomes considerably longer.

From this point of view several different works were contributed in order to reduce complexity and eliminate state space explosion. Ramadge-Wonham worked on discrete event operations and they give some general concept relating to supervision[4]. Rudie and Wonham used decentralized control formulation where specifications are given as global necessities. They apply theory to the problem of reliable transmission of data over a half-duplex channel[5].

Jiang Shebbibg Kumar Rathnesh worked on the decentralized supervisory control problem of concurrent Discrete Event Systems (DES) under partial observation. The result of their framework is the generation of an essential and adequate condition for the presence of decentralized supervisors that provide that the controlled behavior of the systems given between specific range. This result has enabled decentralized control of concurrent systems and decentralized local control settings[6]. Cunha, Cury, and Krogh presents a structure of a consistent abstraction which is an important role in the hierarchical control of discrete event systems[7]. Wong and Wonham built a two-level hierarchy that consists of the high-level and low-level model which connect each other with information channel. They introduced control architecture and use this architecture so as to improve hierarchical consistency and nonblocking condition[8]. Moreover, decentralized and hierarchical control architecture is practiced by Schmidt, Reger and Moor, the authors take into account structural decentralized DES and join together the existing control structure with a two-level hierarchy. For their proposed system, they demonstrate hierarchically consistency and nonblocking condition of the closed-loop behavior[9]. Besides, Schmidt, Perk, Moor worked on the hierarchical control of decentralized discrete event systems that are synchronized by shared events. They ensure hierarchical consistency with a multi-level hierarchical control structure and they reduce the computational complexity of supervisory control synthesis[10].

The approaches suggested by the above-mentioned references are applied individually, and then the approaches are combined and applied to the CBTC system. These approaches aim to reduce system complexity and facilitate controller design. On the other hand, there are several important frameworks about the train signaling system and

interlocking which are worked by Tang, Liu, and Wang present a model-based design approach for CBTC interlocking system using Safety-Critical Application Development Environment (SCADE). Because of the complexity and the safety necessity of CBTC, they proposed an inventive modeling approach to build models of the system[11]. Kaymakci, Anik, Ustoglu focus on interlocking systems in this study. While presenting the discrete event system models of the railway components, they also designed local modular supervisory controllers and checked the controllability and locality conditions[12]. Malakar, Roy modeled railway track interlocking and signalization systems with Automation Petri-Net[13]. Furthermore, formal development and verification of railway control system are worked by Haxthausenand Peleska gives a concept about distributed railway control systems which contain train control computers and switch boxes. In addition, they give information about formal specification and verification that control algorithms performed by the distributed cooperating control components. When it comes to the result of their framework, they eliminate the state-space explosion[14]. Besides formal modeling and verification, the interlocking system is worked by Vu, Haxthausen and Peleska, the authors made a generic updatable model of Danish railway interlocking systems which coherent European Train Control System (ETCS) level 2. As a result, they aim to increase the concurrency level in route allocation and number of the train on the railway. The overcome to state-space explosion problem with Satisfiability Modulo Theories (SMT) which allow high-level safety features[15]. Formal methods for railway control systems worked by Alessandro Fantechi Francesco Flammini Stefania Gnesi focus on information and communication technology related to Intelligent Transportation Systems (ITS) and present formal methods to model and analyze complicated systems in ITS context specifically the railway control system[16]. Many different frameworks about verification of railway interlocking system worked by Kanso Karim; Moller, Faron; Setzer Anton put forward a strategy, which simplicity and it verified safety requirements at the lowest level, of automated verification about signaling basis control of the interlocking system[17]. Lastly, Quian Jie, Liu Jing give basic information about Communications Based Train Control (CBTC). Moreover, they detailed at SCADE system which completes the necessity of design, simulates, verification of safety-critical systems as CBTC. They emphasize in their framework, modeling and verifying CBTC is a challenging problem because of state explosion problem[18]. The above-mentioned studies have not been applied to the CBTC system before. In this study, the aforementioned decentralized hierarchical control architectures are combined and applied to the ATP subsystem of the CBTC system.The steps implemented are as follows: The subsystems that make up the ATP are modeled separately, the controller is designed for each subsystem. Decentralized and hierarchical control architecture has been created for ATP subsystems. Interoperability of the systems has been ensured by establishing a connection between the subsystems. Thus, the modeling complexity encountered in the modeling process of the ATP system was minimized, preventing the state-space explosion and shortening the computation time for controller design. In addition, the condition that the system is not blocked is provided. Critical security protocols (IEEE-1474) are provided for CBTC systems. Moreover, it has been ensured that the subsystems work together without any problems. Finally, a decentralized hierarchical architecture is established and consistency between hierarchical levels is achieved.

In this article, the decentralized hierarchical control system architecture is shown in the following sections, some basic information and notations about CBTC are explained, the controller is synthesized for CBTC. Last but not least, the

results are presented to validate the efficiency of the proposed decentralized hierarchical control architecture composed of sub-systems of CBTC.

2 Decentralized and Hierarchical Control

As the number of subsystems in a plant increases, system complexity increases. Therefore, it is very difficult to model these systems and design their controllers with a monolithic approach. With the decentralized and hierarchical approach, the problems encountered in the monolithic approach disappear. In this way, modeling of the system and controller design can be made more easily.

2.1 Monolithic Supervisory Control Approach

Monolithic audit control faces the problem of very high computational effort for large systems. In this approach, the system is not divided into any subsystems and is taken as a single unit. The model is created considering all the states of the subsystems of the system and a controller design is made according to this model. Considering system as a single unit, the supervisory observer synthesis calculation obtained becomes very complex. The reason being the structure of system, which has a large number of components. As the number of components increases, the state space increases exponentially and the state space explosion occurs. The monolithic model of the ATP system can be seen in Figure.1. There are 87 cases in the monolithic model. As can be understood from Fig.1, the system model is quite complex in the monolithic approach. It is very difficult to design a controller for this model. The model shown in Fig. 1 is only for the ATP. Since it consists of many subsystems such as CBTC, ATO and ATS, it is obvious how complex the model to be obtained with the monolithic approach by considering these subsystems.

2.2 Decentralized Control Architecture

The decentralized control architecture separates a plant, which consists of the subsystems, to the subsystems. For all separated subsystems, specifications are defined individually. In order to ensure these specifications, individual supervisors are synthesized. As all subsystems are coupled with each other, in order to have a plant model from a subsystem, the synchronous product is used of all subsystems. This is suggested by Lee and Wong[19].

2.3 Hierarchical Control Architecture

In hierarchical architectures, supervisor synthesis is based on a plant abstraction. The abstracted plant is called a high-level model. A low-level model is more complex than the high-level model and the original plant model represents the low-level model. Technically, abstractions can be made with natural projections. Natural projection is a very important process on how to obtain the plant abstraction, such a high-level controller can be performed by existing the low-level control activity. In other words, this is hierarchical consistency. At this point how will hierarchical consistency ensure? The answer to this question is given by Zhong and Wonham[20]. The decentralized control system, the plants are

separated into the subsystem and these separated subsystems have their individual supervisors. The system behavior can be expressed with the alphabet and automata.

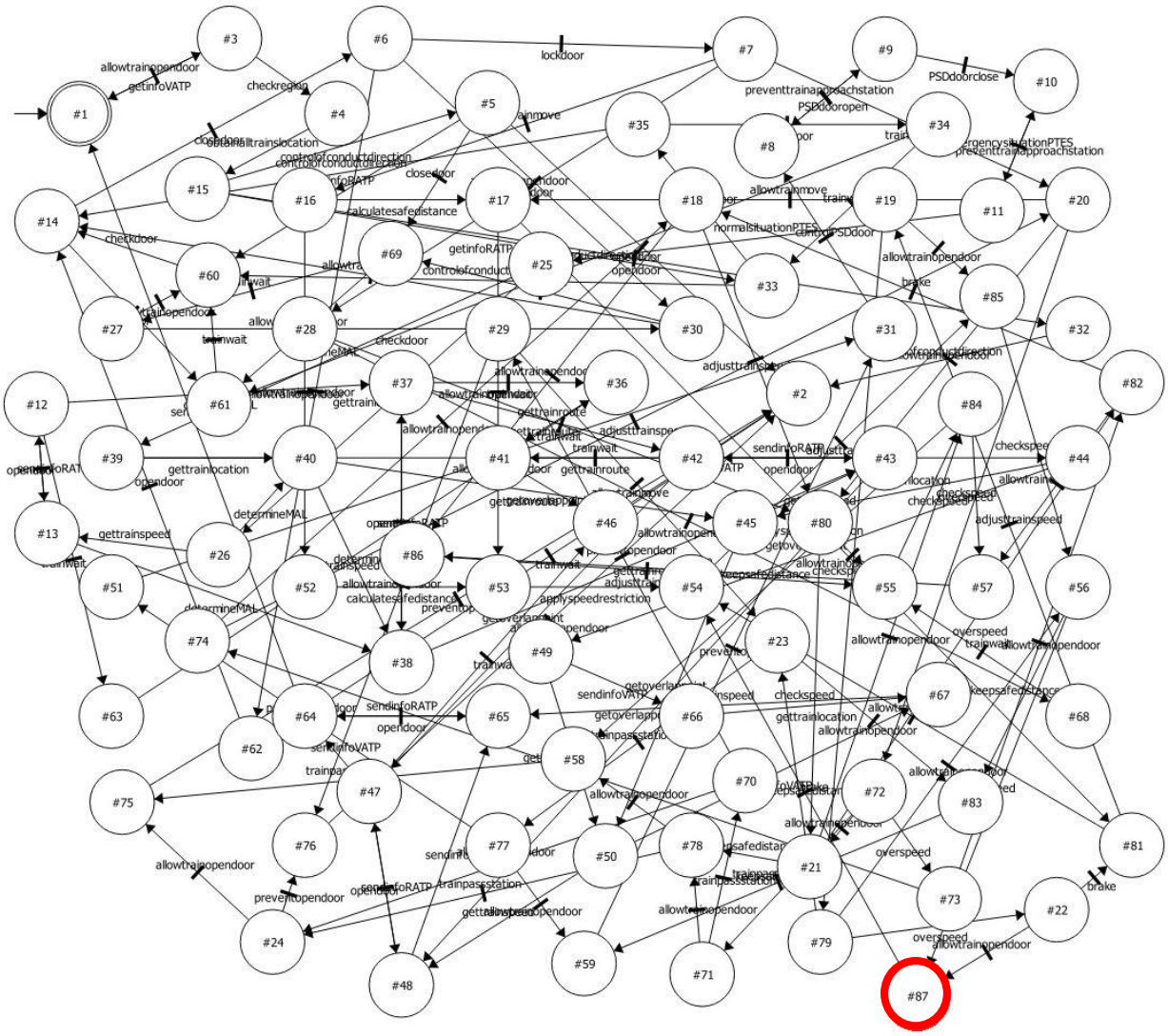

Fig. 1. Monolithic model of ATP subsystem

The alphabet is denoted by Σ and the automata is denoted by G. The finite-state automata can be modeled as G_i , $i = 1,2 \ldots\ldots, n$. All subsystems have alphabet which is represented with Σ_i , $i = 1,2 \ldots\ldots, n$. The whole systems are defined as $G \coloneqq G_1 || \, G_2 || \ldots\ldots || G_n$ or $G \coloneqq ||_{i=1}^{n} G_i$ over the alphabet $\Sigma \coloneqq \Sigma_1 \cup \Sigma_2 \cup \ldots\ldots \cup \Sigma_n$ or $\Sigma \coloneqq \cup_{i=1}^{n} \Sigma_i$. Also, we can write the controllable and uncontrollable events $\Sigma_{i,c} \coloneqq \Sigma_i \cap \Sigma_c$ and $\Sigma_{i,uc} \coloneqq \Sigma_i \cap \Sigma_{uc}$ where $\Sigma = \Sigma_c \cup \Sigma_{uc}$ and $\Sigma_c \cap \Sigma_{uc} = \emptyset$. The separated subsystems like G_i, G_j are synchronized with shared events only if $\Sigma_i \cap \Sigma_j \neq \emptyset$.

The local low-level supervisor is denoted by $S_i : L_i \rightarrow \Gamma_i$ (Γ_i control pattern). The Low-level closed-loop languages $L_i^c \coloneqq L(S_i/G_i)$ $L_{i,m}^c \coloneqq L_i^c \cap L_{i,m}$, $L^c \coloneqq ||_{i=1}^{n} L_i^c$, $L_m^c \coloneqq ||_{i=1}^{n} L_{i,m}^c = L^c \cap L_m$.

$L^c = L(G^c),\ L_m^c = L_m(G^c)$ where G^c is a generator. On the other hand, the projected low-level system's supervisor or high-level system's supervisor is denoted by $S^{hi}: L^{hi} \rightarrow \Gamma^{hi}$ and high-level closed-loop language $L(S^{hi}/G^{hi})$. An available low-level supervisor $S^{lo}: L^c \rightarrow \Gamma$ entail to execute $\theta(L(S^{lo}/G^c)) \subseteq L(S^{hi}/G^{hi})$.

Eventually, hierarchical abstraction obtain with the reporter map (natural projection) $\theta: \Sigma^* \rightarrow (\Sigma^{hi})^*$ and $\Sigma^{hi} \coloneqq \cup_{i,j,i\neq j} (\Sigma_i \cap \Sigma_j)$. The high-level language obtain with $L^{hi} \coloneqq \theta(L^c)$ and $L_m^{hi} \coloneqq \{s^{hi} \epsilon\ L^{hi}\ s.t. \theta^{-1}(s^{hi}) \cap L_m^c \neq \emptyset$ and G^{hi} such that $L^{hi} = L(G^{hi})$.

From this perspective, we can amalgamate the hierarchical control system with a decentralized control framework. Finally, the hierarchical and decentralized control system's architecture is obtained. Fig. 2[10] demonstrates the structure of hierarchical and decentralized control.

In the shown model, S denotes for supervisory controllers while G denotes for the system's behavior, expressed by finite state automata. Other symbols include; Com for command, Con for controller, Inf. for information, hi for high-level systems, lo for the low-level systems. Their functions are demonstrated below:

- Com_hilo→ Denotes for sending commands from the upper-level supervisory observer to the lower-level supervisory observer.
- Inf_lohi→ Denotes for sending information from the lower level system to the higher level system.
- Con_hi→ Denotes for sending commands to the higher level system by the upper level supervisory observer.
- Inf_hi→ Denotes for sending information from the top level system to the top level supervisory observer.
- Con_lo→ Denotes for sending commands to the lower level system by the lower level supervisory observer,
- Inf_lo→ At the lower level, it refers to sending information from the lower level system to the lower level supervisory observer.

These parameters ensure interoperability of the system as well as coordination between systems. In this way, the sub-systems communicate among themselves and the upper-level system models are obtained while ensuring the interoperability of the lower-level and upper-level systems. [10].

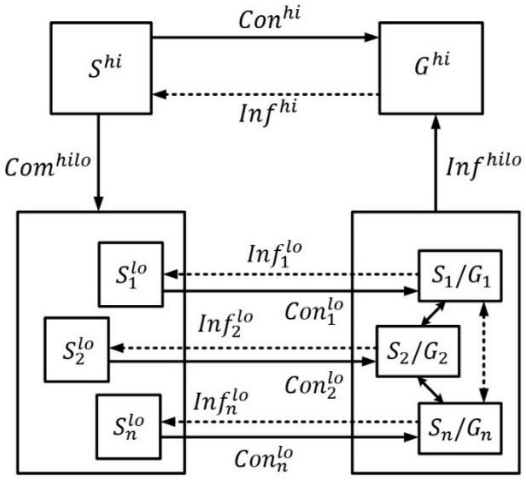

Fig. 2 Hierarchical and decentralized control architecture

3 Communication Based Train Control System (CBTC)

The Communication Based Train Control signaling system communicates with the wireless data transfer between the train center and the trains on the rail line and provides uninterrupted and instant information exchange. Thanks to the communication, the exact position, speed and remote control of the trains on the rail line can be explained as signaling systems that make the train more accurate and faster than fixed blocking signaling systems. CBTC is equipped with continuous, high-capacity and bi-directional information exchange.

In CBTC, the track line is divided into virtual blocks. As trains move through these virtual blocks, they constantly generate signals in front and behind. These signals move along with the train. By way of example, let's assume that the two trains move on the track. From these two trains, the leading train is slower and the rear train is moving faster. When the signals of the front train coincide with the signals of the rear train, the rear train adjusts its own speed relative to the front train and continues its course at a safe distance. Compared to traditional systems, the CBTC makes trains and train control faster and more accurate.

The CBTC system basically has the following components.

- Automatic Train Supervision (ATS)
- Automatic Train Protection (ATP)
- Automatic Train Operation (ATO)

Optionally, for autonomous train control, ATO is used. ATS, ATP and ATO standards are determined according to IEEE- 1474. Both ATP and ATO consist of two different subsystems. ATP has Vehicle Automatic Train Protection (VATP) and Regional Automatic Train Protection (RATP). Similarly, ATO also has Vehicle Automatic Train Operation (VATO) and Regional Train Operation (RATO). All of these subsystems have specific tasks.

ATS system monitors trains and regulates the performance of individual trains to organize programs. The other task of ATS is scheduling train traffic.

The Automatic Train Supervision system is responsible for monitoring train activities to ensure that trains act in accordance with the traffic order within the specified itinerary. However, ATS has different tasks in the system. These tasks are the evaluation of route design requests, monitor ATP and ATP status, generate statistics and reports related to systems also train, monitor system status, evaluation of switch status and allocation of switch and prohibiton of the route according to route status respectively.

The Automatic Train Protection system is a very important system that is responsible for ensuring the safe movement of trains. ATP ensures safe movement between trains. In doing so, it applies speed limits to ensure that the train operates within safe movement limits. If a train exceeds the speed limits, the ATP is engaged and automatically brakes to stop the train or move it within safe speed limits.

ATP subsystem prevents collisions from accidents due to a fault or speed restrictions. ATP monitors the train, also it controls the train speed and it can brakes if necessary. ATP consists of two subsystems Vehicle Automatic Train Protection (VATP) and Regional Automatic Train Protection (RATP).

On-Board ATP receives the route, overlap point and speed constraints it needs from the Regional ATP. The onboard ATP is located on the train and performs the following functions; detection of the position of each train on the line,

maintaining a safe distance between moving trains, applying speed restrictions to the moving train, braking on the train if the perceived train speed exceeds the specified train speed, monitor the status of train doors which check and ensure train doors closed and locked, allowing the train departure according to the status of the train gates, preventing the opening of train doors if the train passes the station, preventing the entrance of the train to the station when the platform separator doors are open.

The regional ATP train receives location, speed and direction information from the On-Board ATP. The regional ATP is located along the line within the designated regions and performs the following functions; detection of the positions of each train on the line, the important task of RATP is the determination of the movement authority limit (MAL), checking the normal direction of course, monitoring of closing and locking of train doors, preventing trains from entering the platform when the platform separator door is open, allowing train departure according to the status of the train gates.

The Automatic Train Operating System is responsible for the machinist's functions. ATO provides the train to depart smoothly during departure and to stop the train so that it does not shake the passengers by soft braking while braking. Conventionally, it is responsible for the traction power of the train and for braking commands. It is also responsible for the correct stop of the train at the station and the opening and closing of the doors. The train transmits speed data to the ATO while it is traveling and enables the acceleration and braking functions to be adjusted according to this speed data. Namely, ATO subsystem task is to operate the train without a driver, such as starting and stopping the train, energy-efficient braking and ensure smooth acceleration, and stopping at the destination accuracy. ATO also consists of two subsystems Vehicle Automatic Train Operation (VATO) and Regional Train Automatic Operation (RATO).

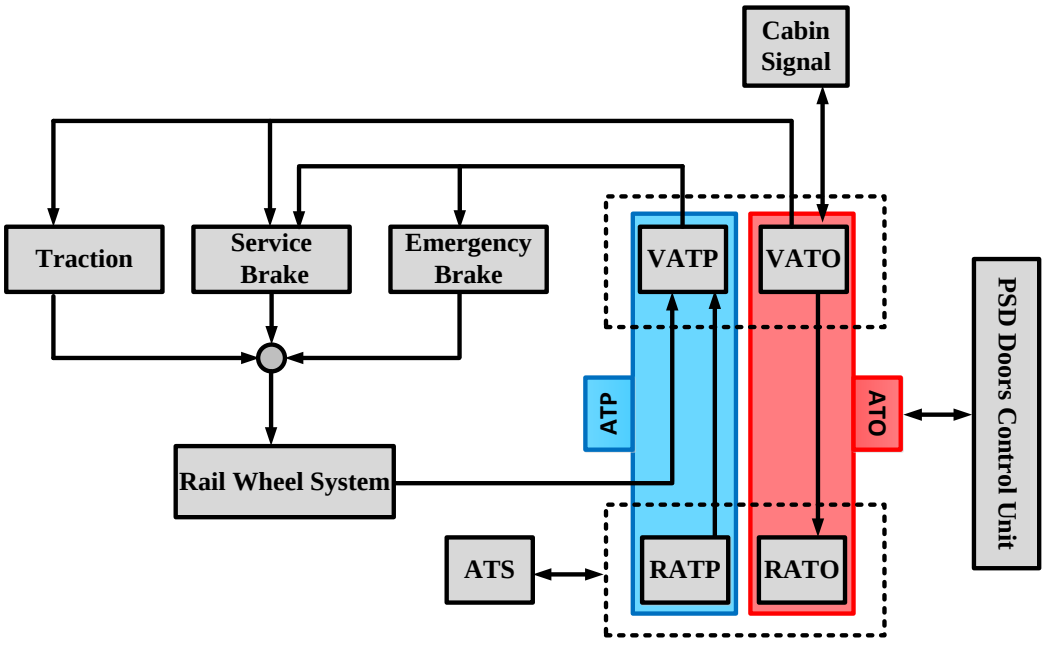

Fig. 3 CBTC architecture

The onboard ATO is located on the train and the VATO system performs the following functions under the control of the VATO system; command output to train braking system, closing the passenger door and detecting its status, control of opening and closing of platform separator door systems, returning at end-of-service stations, activation and commissioning of parked trains, parking of the trains that finished the expedition to the parking areas, command output to the propulsion system for automatic activation of the train, providing command output to the propulsion and braking system for setting acceleration, speed, and idle levels according to driving strategies, communication with regional ATO.The regional ATO is located along the track at the designated points on the track and performs the following functions; communicate train information to the regional ATP, check the target and adjustment targets of each train.The basic structure of CBTC can be seen in Fig. 3. There are many advantages of moving block when compared with fixed block. Some of the important advantages: the rail track occupation is severely reduced. The rail tracks are used more efficiently. Moreover, it provides easy maintenance, easy integration, easy expansion and it needs minimum trackside equipment. CBTC can be integrated with automation systems for railway transport easily. Besides, it gives higher operational availability with severe flexibility of train action[11], [21]–[23].

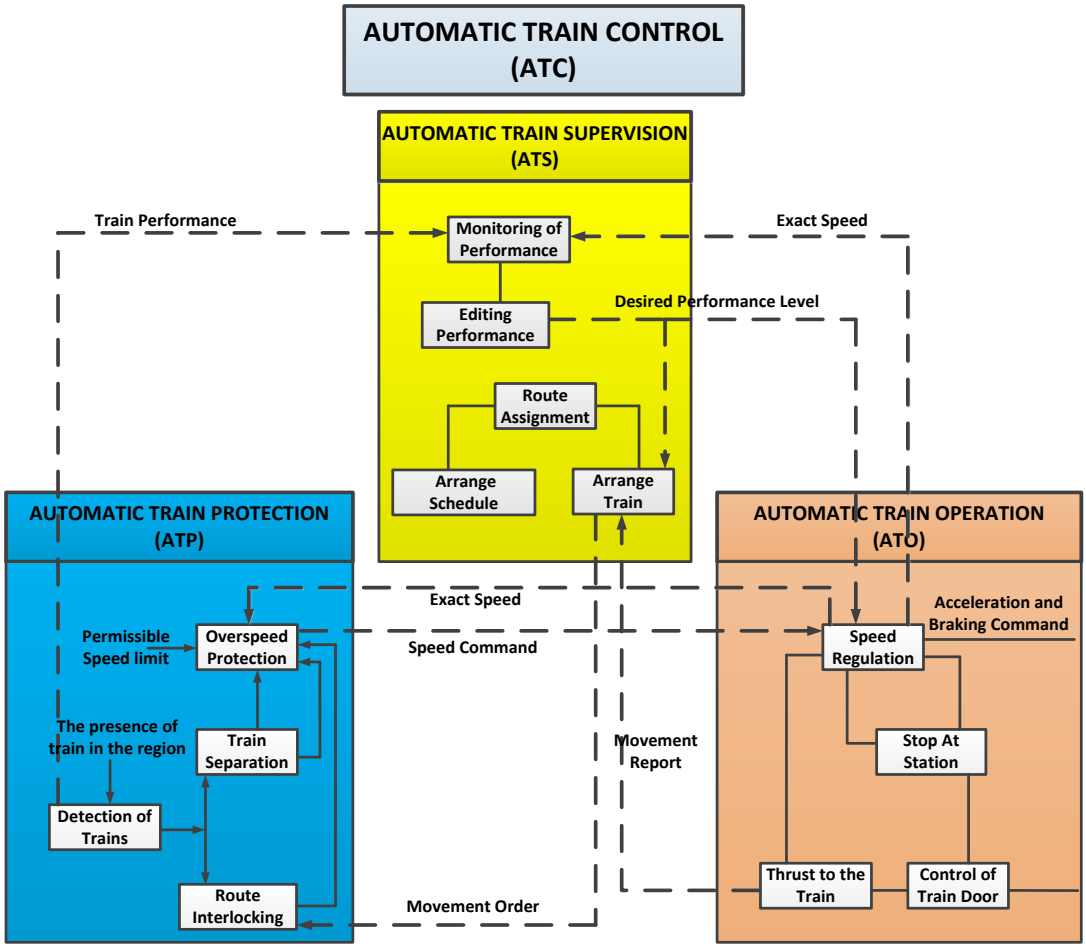

Fig. 4 Automatic Train Control Structure

The relation of CBTC subsystems and operating principles for exchanged data and information can be seen in Fig. 4. If we extend the title a little more, ATP sends train performance data to ATS, when ATS get these data, ATS evaluate these data and editing train performance using the data. The edited performance information is sent to the ATO to bring the train to the desired performance level. When ATO get information from ATS, it makes necessary arrangement related to speed regulation. Besides, ATO send exact speed info to both ATP and ATS, it gets speed command data about the train's speed from ATP. Furthermore, ATO sends movement reports to ATS to make arrangements related to train and ATS send movement order information to the ATP.

The picture above shows the relationship between the CBTC subsystems. Thanks to the exchange of information between them, the systems provide the interoperability feature seamlessly while ensuring the reliable operation of the systems and the train by fulfilling the reliability conditions of the rail line and other systems on the rail line.

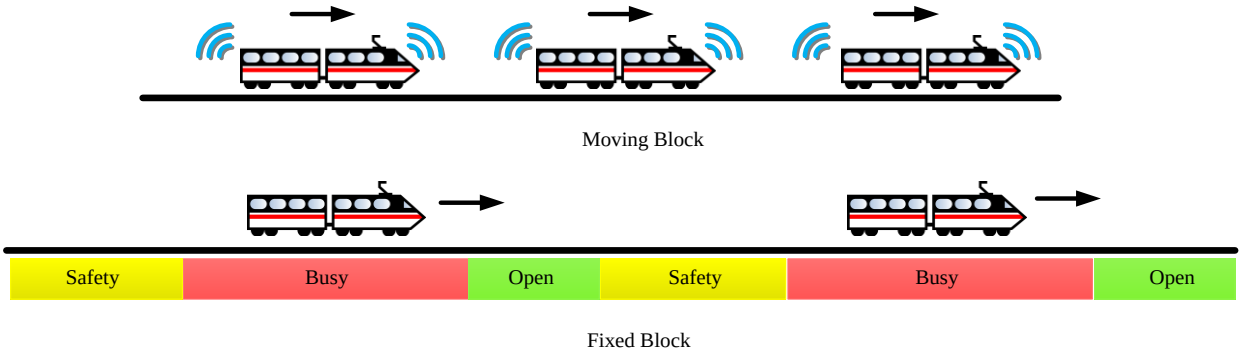

Fig. 5 Moving block vs fixed block

A comparison of the fixed block and the moving block is shown in Fig. 5. Track line is divided into the virtual block in the CBTC systems, which all trains always communicate with each other via regional subsystem and these trains adjust their speed and distance very quickly. Whereas in fixed block, the track line divided the real block and only one train allowed to occupy one block. Moreover, there is no need for any color lights signals with a moving block, but for classic fixed block color lights signals is very important for regulating train traffic and ensure safe movement[21], [22], [24].

4 Modeling of CBTC with Finite State and Decentralized-Hierarchical Control of CBTC

After a general overview of CBTC, all CBTC systems are separated into the subsystems. This section focuses on modeling. At first, low-level model of ATP is modeled. ATP has two sub-systems that are VATP and RATP. In this study, there are two model type which called the low-level model and the high-level model. The low-level model also called a detailed model, which include all possible behavior of the systems. The high-level model is the projection of controlled behavior of the low-level model, and it is less complex than the low-level model. Another important term is the specification. The specifications indicated the desired behavior of the systems and it is defined depending on the systems. In this study the specifications are defined for VATP and RATP. Using with defined specification for VATP, RATP subsystems and low-level model of the VATP, RATP subsystems, the supervisor of the low-level ATP model is synthesized. After obtained a supervisor, shared events for common events that occur between subsystems are defined. With natural projection operation and using shared events, a high-level model is obtained. Finally, the decentralized-

hierarchical architecture is built with the low-level model, the high-level model, the low-level supervisor and the high-level supervisor. Furthermore, the other subsystems can be modeled in the same way as the ATP model as we mentioned above. In this study, the VATP model is presented in detail. RATP high-level model is given below for parallel composition process. The result of implementing the parallel composition operation is obtained for all subsystems to work together. The following nomenclature is used for modeling the ATP system and obtain a supervisor of the ATP. Another way is finite alphabet is denoted by Σ for describe system behavior. The set of all finite strings which is systems behavior is represented by Σ^* which is also known as Kleene Closure. Let L is a language over Σ alphabet, L is a subset of Σ^* and ($L \subseteq \Sigma^*$). The prefix closure of L is denoted by $\bar{L}$. and $\bar{L}$ comprise of all the prefixes of all the strings in L[20]. The low-level uncontrolled model of VATP(G^0_{VATP}) can be seen on Fig. 6. Here in Fig.6, some transitions have a bar and some transitions do not have this bar. This bar means that whether the events are controllable or not. If any transition has a bar this means this event is controllable and if not it is not controllable. The supervisor is only capable to control controllable events. The explanation of the events of all models is given in Table-1 below.

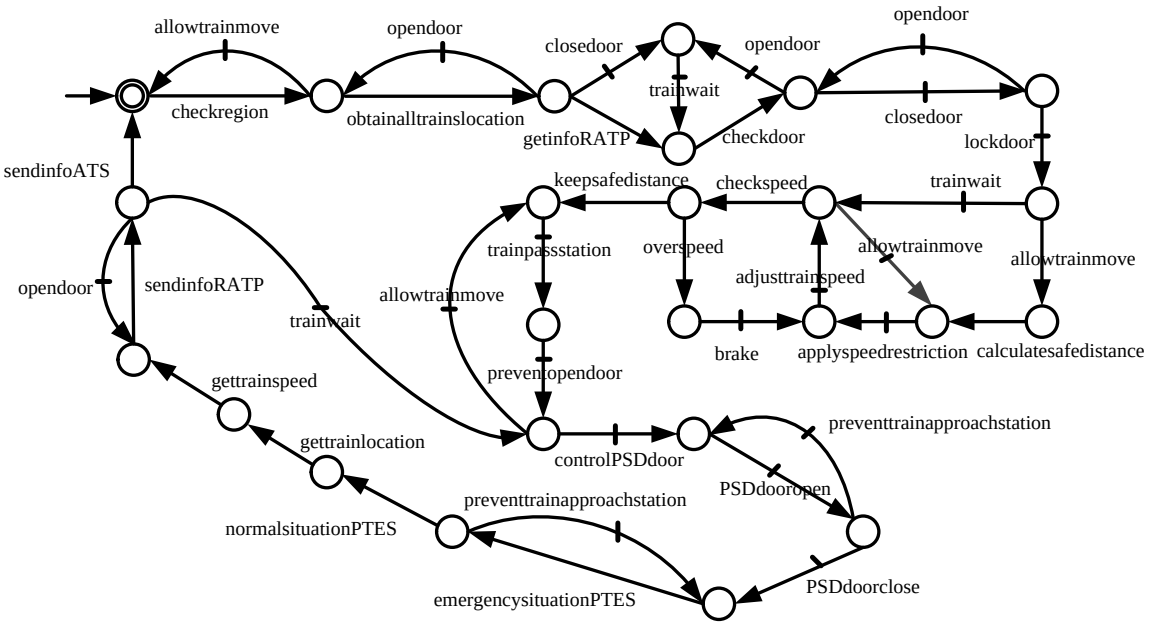

Fig. 6 Low-level and uncontrolled model of VATP(G^0_{VATP})

Fig. 6 shows the VATP system's uncontrolled behavior. In other words, there is unwanted behavior in the uncontrolled model. In the model in Fig. 6, the movement of the train was allowed after the virtual zones were checked. The fact that the movement of the train is allowed after virtual zone control is undesirable. Therefore, the models involving such behavior are called uncontrolled models. The following examples can be given to uncontrolled behavior: train over speed, the brakes don't react while a train is coursing, etc. When such unwanted behavior happens, the system cannot work properly. So as to bring this uncontrolled model to controllable model; the two conditions needs to be met can be given as in Fig. 7.

The two specifications are defined for VATP. The first specification is defined for train doors situation which is related to door and train movement relation and the second one is defined for preventing collision on track line. The purpose of this specification is to learn the train locations after the control of the virtual zones and adjust the speed of train according to the speed of the other trains and send this information to RATP and ATS.

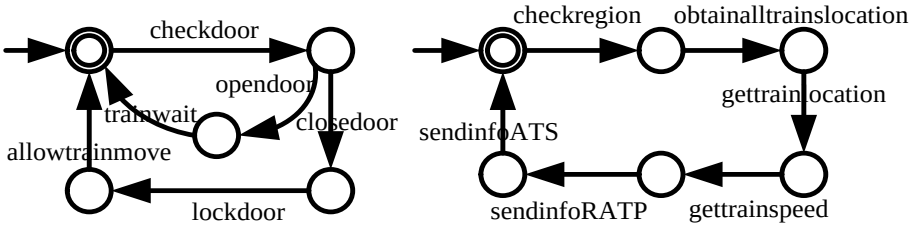

Fig. 7 Specification for VATP (D^0_{1VATP}, D^0_{2VATP})

There are specifications for the VATP system to perform certain tasks. With these specifications, controllers will be synthesized to minimize the unwanted behavior of the system. These specifications are combined with the parallel composition process and parallel composition can express with mathematical as $L_1 \,||\, L_2 \subseteq \Sigma^*$. This operations model two forms of joint behavior of a set of automata that operate concurrently.

$D^0_{VATP} = D^0_{1VATP} || D^0_{2VATP}$

In this instance, one should remember that supervisor basically restricts the behavior of an uncontrolled model which low- model VATP (G^0_{VATP}), in order to satisfy specified specification related to the system. Supervisor denoted by S. Supervisor S produce close-loop behavior $\kappa_{L(G)}(D)$ that means maximal permissive behavior. A specification language D is L_m-closed if $\bar{D} \cap L_m = D$. $L_m(G)$-closed languages set is shown with $\mathfrak{F}_{L_m(G)}$. Whether a specification D element of $\mathfrak{F}_{L_m(G)}$, then the plant generated language $L(G)$ is non-blocking under maximal permissive supervision. E is said to be a controllable language with respect to $L(G)$ that ensured that there is a supervisor S so that $\bar{E} = L(S/G)$. The set of all controllable language is represented by $C(L(G))$ and $C\big(L(G)\big) = \{E \subseteq L(G) | \exists S \; such \; that \; \bar{E} = L(S/G)\}$. Hence, for entire specifications language D, a supremal controllable sublanguage of D is existed with respect to $L(G)$. Supremal controllable sublanguage of D is defined as $\kappa_{L(G)}(D) \coloneqq \cup \{K \in C\big(L(G)\big) \,\big|\, K \subseteq D\}$.

The K language is defined as the language set that expect the system to exhibit the desired behavior under its supervisor. However, the K language containing the expected behavior of this system may not be controllable. If K is not controllable, the system cannot display the desired behavior. Controllable sub-languages of the language may be used for the design of supervisory observers that will give the expected behavior. Of these languages, the largest controllable K is called the largest controllable sub-language which indicated by $K^{\uparrow C}$.

The supervisor of VATP are synthesized with the structure below. The model of the supervisor of VATP can be seen as in Fig. 8.

$$L(S^0_{VATP}/G^0_{VATP}) = \kappa_{L(G^0_{VATP})}(D^0_{VATP})$$

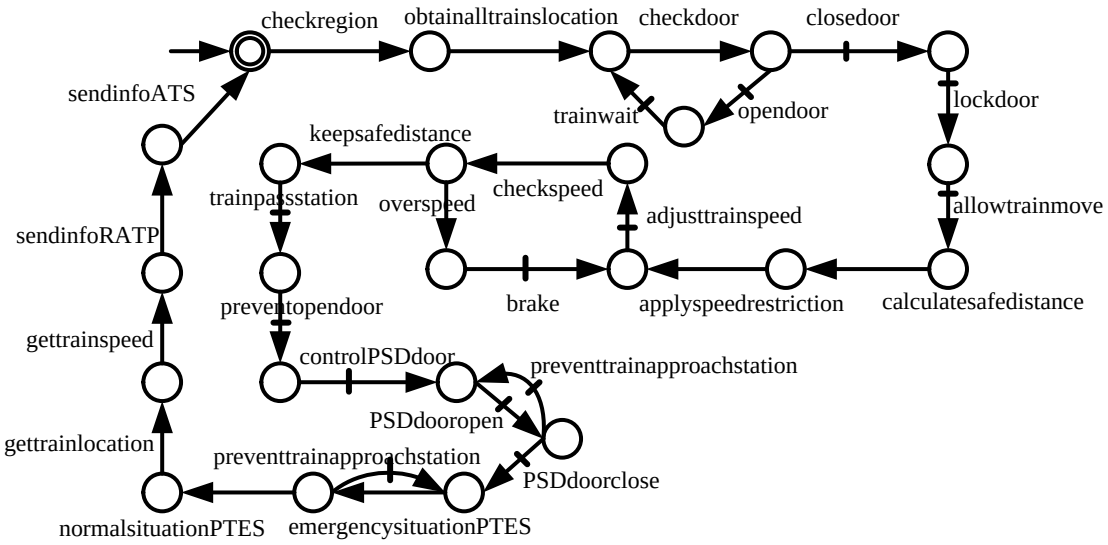

Fig. 8 Controlled behavior of VATP (Supervisor) ($G_{VATP}^{(0),c}$)

Using the specifications at Fig. 7 and the uncontrolled model at Fig. 6. The controlled model of the VATP system which supervisor of VATP is obtained. This controller observe the systems and disables some events, which are controllable. The VATP sub-system is connected to the RATP sub-system via the shared events. For having a high-level VATP model the shared events are specified as below definition.

$\Sigma_{VATP}^{1} = \{getinfoRATP, senfinfoRATP, sendinfoATS, controlPSDdoor\}$ and $\Sigma_{VATP}^{1} \subseteq \Sigma_{VATP}^{0}$

Natural projection is used in order to obtain a high-level model. The natural projection can basically be explained as follows. It deletes events that do not belong to the smaller event set (Σ_s) from the larger event set (Σ_l). Σ_l and Σ_s represent larger and smaller event set respectively.

After obtaining the controlled model, the events shared with other systems are determined and the high-level model of the VATP is obtained. While obtaining a high-level model, the natural projection process is used. The high-level model of VATP can be seen at Fig. 9.

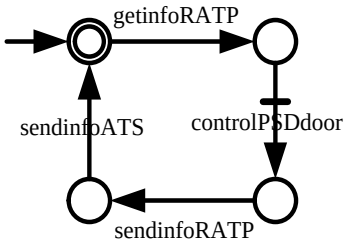

Fig. 9 High-level model of VATP (Projected Model) ($G_{VATP}^{(1),c}$)

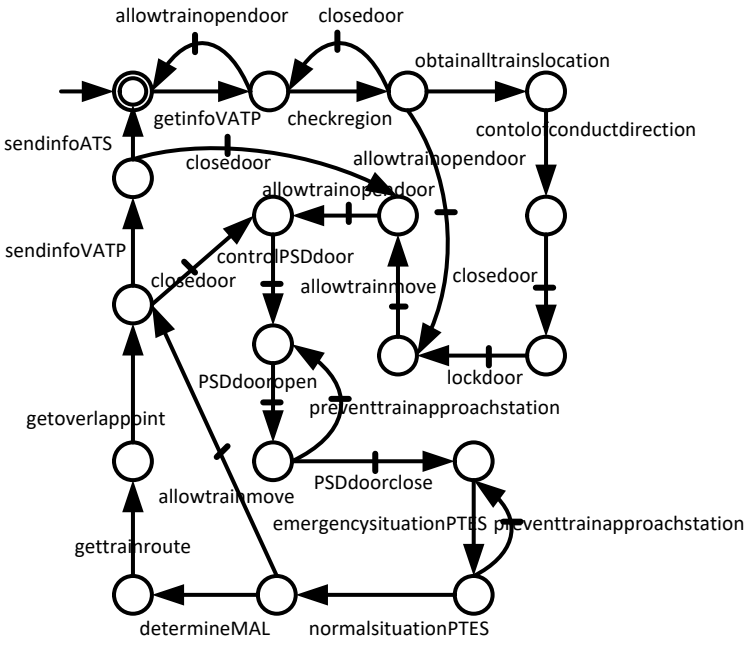

Fig. 10 Low-level and uncontrolled model of RATP(G^0_{RATP})

The same operations applied to the VATP subsystem are also applied to the RATP subsystem. First, the low-level model of RATP Fig. 10 is defined and modeled with finite state automata.

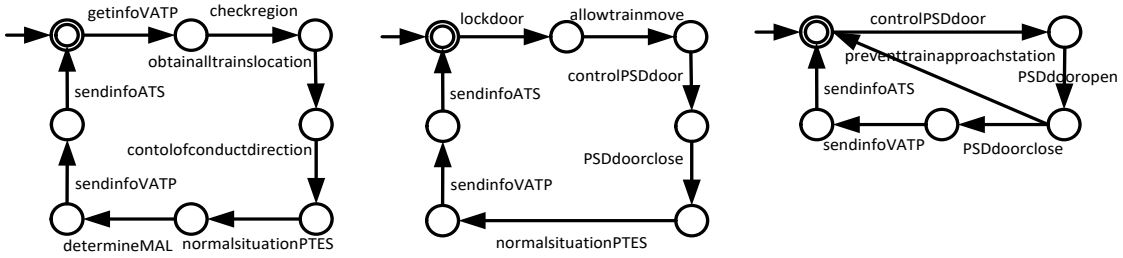

Fig. 11 Specification for RATP ($D^0_{1RATP}, D^0_{2RATP}, D^0_{3RATP}$)

Second, the specification is defined for RATP Fig. 11. The general model of the RATP is obtained with parallel composition which include the three specifications.

$D^0_{RATP} = D^0_{1RATP} || D^0_{2RATP} || D^0_{3RATP}$

Eventually, the controlled behavior that is low-level supervisor of the RATP subsystem is obtained with the uncontrolled behavior of RATP and the defined specification of the RATP. The following equation is defined for obtain to the supervisor of RATP sub-system.

$L(S^0_{RATP}/G^0_{RATP}) = \kappa_{L(G^0_{RATP})}(D^0_{RATP})$

The supervisor model of the low-level RATP sub-system can be seen at Fig. 12.

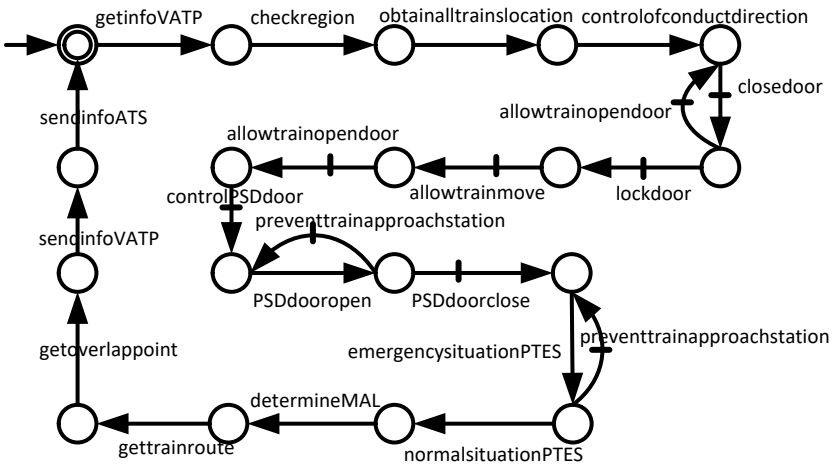

Fig. 12 Controlled behavior of RATP (Supervisor) ($G_{RATP}^{(0),c}$)

In the same way, the shared events are specified for having a high-level RATP subsystem as following. $\Sigma_{RATP}^{1} = \{getinfoVATP, senfinfoVATP, sendinfoATS, controlPSDdoor\}$ and $\Sigma_{RATP}^{1} \subseteq \Sigma_{RATP}^{0}$ with shared events and natural projection, the high-level model of RATP is obtained. The high-level model of the RATP subsystem can be seen as Fig. 13.

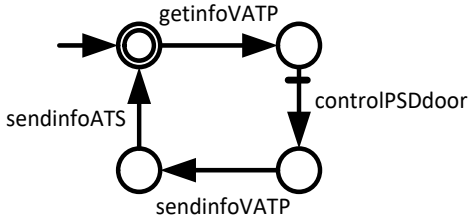

Fig. 13 High-level model of RATP (Projected Model) ($G_{RATP}^{(1),c}$)

The high-level models of VATP and RATP are used for synchronization. With the parallel composition process, the high-level model of the ATP system Fig. 14 which includes VATP and RATP is obtained. The following equation is defined for parallel composition of the high-level VATP and the high-level RATP subsystems. Fig. 14 is the model of high-level ATP systems.

$$G_{ATP}^{1} = G_{VATP}^{1} || G_{RATP}^{1}$$

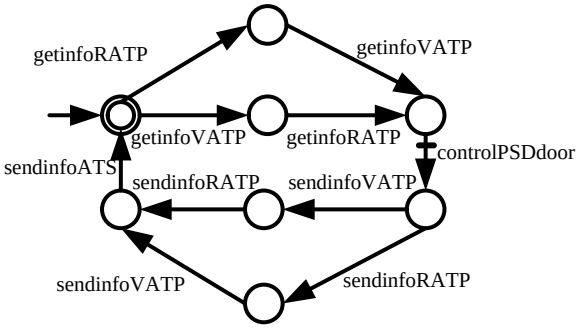

Fig. 14 Parallel composition of RATP and VATP (G_{ATP}^{1})

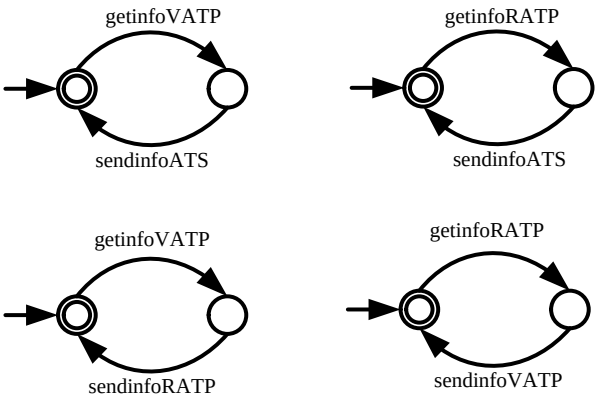

Fig. 15 Specification for synchronous high-level subsystems ATP

For synchronous high-level subsystems Fig. 14, the specifications are defined respectively as D^1_{1ATP} , $D^1_{2ATP}, D^1_{3ATP}, D^1_{4ATP}$.

$D^1_{ATP} = D^1_{1ATP}||D^1_{2ATP}||D^1_{3ATP}||D^1_{4ATP}$

Supervised behavior of synchronous high-level subsystems is calculated with following equation.

$L(S^1_{ATP}/G^1_{ATP}) = \kappa_{L(G^1_{ATP})}(D^1_{ATP})$

Supervised behavior is also called as controlled behavior or supervisor. The supervisor model of ATP can be seen at Fig. 16. When Fig.14 and Fig.16 areconsidered, it is seen that Fig.14 and Fig.16 are the same. This is because of the specifications which has been defined. The supervisory controller that provides the system specifications is Fig.16.

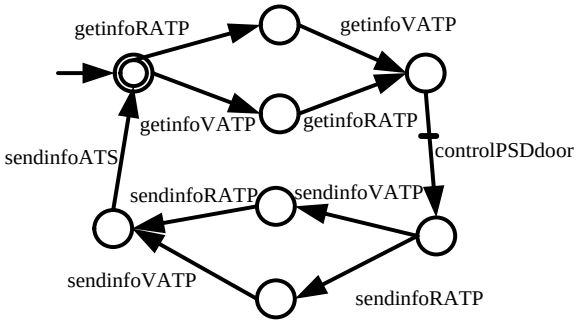

Fig. 16 Controlled behavior of VATP-RATP (Supervisor)($G^{(1),c}_{ATP}$)

The top of the hierarchy can be obtained with the same calculation, and it can be seen at Fig. 17.

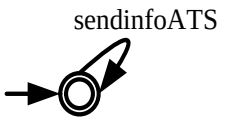

Fig. 17 High-level-2 model of VATP-RATP (Projected Model)($G^{(2),c}_{ATP}$)

The supervisory controllers (Fig.8, Fig.12) and the upper-level models (Fig.9, Fig.13) of the VATP (Fig.6) and RATP (Fig.10) subsystems have been successfully obtained, as can be seen above. Undesirable situations in the system will be prevented due to supervisory controllers. Therefore, the system will work safely and meet the security requirements. Since we divide the systems into subsystems, interoperability of the systems is also provided by the parallel composition process. The parallel composition process was performed using the upper level-1 VATP and RATP models obtained and the two subsystems were combined with this process. The specifications for this VATP-RATP model are defined and the supervisory controller is obtained with this specification and the VATP-RATP model. In the obtained VATP-RATP model, unwanted situations will be prevented by the supervisory controller. As a result, the interoperability of the systems has been ensured safely.

After all the decentralized and hierarchical structure is constructed with all defined low-level model and obtained supervisor of the sub-systems which are VATP and RATP, the high-level model of the VATP and RATP.

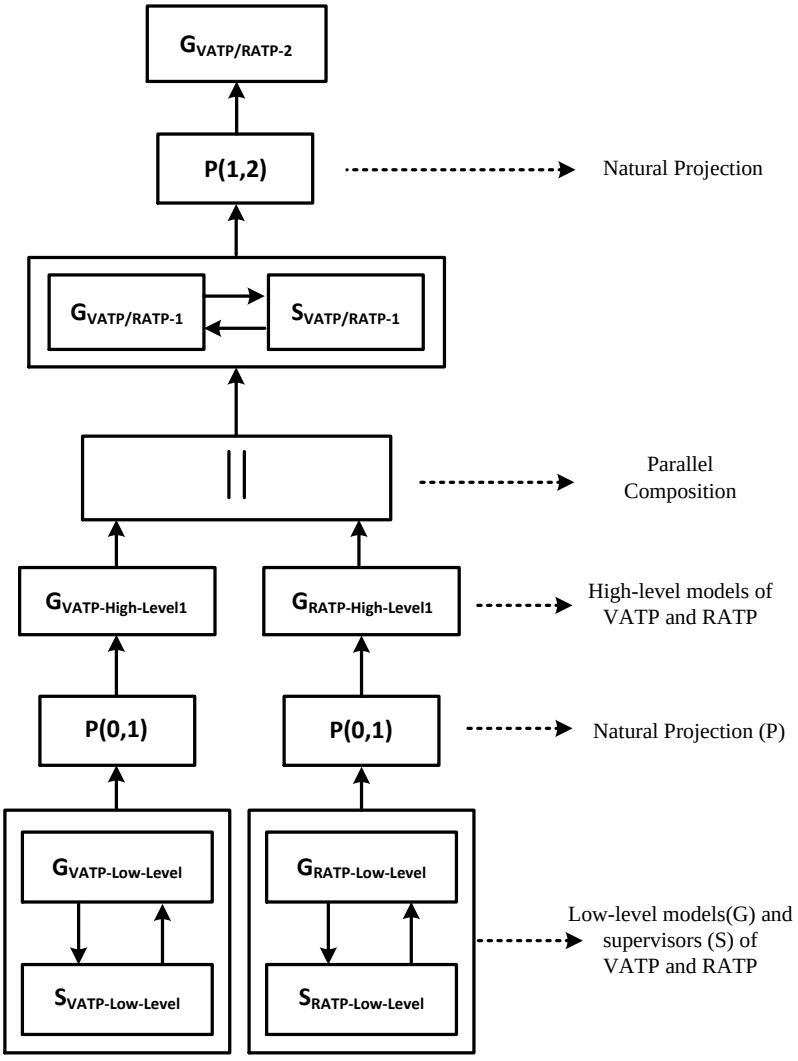

Fig. 18 Decentralized-hierarchical control of VATP-RATP subsystem

The decentralized-hierarchical control of VATP-RATP subsystem can be seen at Fig.18. Here, supervisory controllers $S_{RATP-Low-Level}$ and $S_{VATP-Low-Level}$were synthesized using models and specifications of lower-level systems $G_{VATP-Low-Level}$ and $G_{RATP-Low-Level}$. The letter P indicates the projection process. With the projection process, $G_{VATP-High-Level-1}$ and $G_{RATP-High-Level-1}$) were obtained. In addition, parallel composition process (||) was performed to ensure the interoperability of high-level models and $G_{VATP-RATP-1}$ was obtained. The same procedures were repeated until the highest level $G_{VATP-RATP-2}$ was obtained. The decentralized-hierarchical structure is established with the models described above and the obtained supervisors, the obtained high-level models.The events, which are used for modeling ATP systems, are defined at Table 1.

Table 1 Explanation of events

Events	**Definition**
adjusttrainspeed	Adjust of train speed
allowtrainmove	Train can move
allowtrainopendoor	Train door can be opened
applyspeedrestriction	Train speed regulate
brake	Train must brake
calculatesafedistance	Prevent to train from collision
checkdoor	Checking whether the doors of the train are open
checkregion	Checking of the separated virtual area
checkspeed	Checking of train safety speed
closedoor	Close the train door
controlPSDdoor	Control of platform separated door
determineMAL	Movement Authority Limit
emergencysituationPTES	Push the emergency situation button
getinfoRATP	Take train and region information from RATP
getinfoVATP	Take train information from VATP
keepsafedistance	The train keeps its position at safe
lockdoor	Train door lock
normalsituationPTES	No emergency situation
obtainalltrainslocation	Monitor all train at track line and get the location of trains
opendoor	Open the train door
overspeed	Information of exceeding of the train speed limit
PSDdoorclose/PSDdooropen	Close/Open platform separated door
preventopendoor	Prevent opening of the train door
preventtrainapproachstation	Prevent train enter to the train station
sendinfoATS	Send train and track information to the ATS
sendinfoRATP	Send region and train information RATP
sendinfoVATP	Send train information VATP
trainpassstation	Train does not stop at the station
trainwait	Train does not move

5 Conclusion

In this study, CBTC and its subsystems which ATS, ATP, and ATO is discussed in general terms. The IEEE 1474 standard which included enhancing and improve performance, operations, availability and, train protection is taken into account.

The CBTC system, which has a very complex structure, is divided into sub-systems. Mathematical calculations for sub-systems are presented. Thus, these subsystems from low level to high level are modeled. The controllers for each low-level model and high-level model are designed. As a result, the system model is simplified by minimizing the explosion of state space and considerably shortened the time required for the controller design.

VATP and RATP are modeled with finite state automata, moreover, the controller is synthesized for the VATP and RATP individually. ATP model is obtained with VATP and RATP The supervisory controller of the ATP system is obtained both monolithic approach and the decentralized-hierarchical control approach. As a result of the monolithic approach, the state space of the system is obtained bigger than the decentralized-hierarchical control approach. In the monolithic approach, VATP and RATP have 87 states. When the other subsystems of the CBTC which are ATO and ATS included in the process, a state-space explosion occurs and it becomes difficult to track states, while the controller design of this model becomes very difficult and the calculation time of controllers takes too long.

In the decentralized-hierarchical control approach, VATP-RATP state numbers are calculated as only 48 states. Any other way, if compared to the monolithic approach, with the decentralized-hierarchical control approach, the latter approach reduce system complexity and state-space explosion. The other benefits of decentralized-hierarchical control, reducing complexity and calculation times.

Another vital issue, interoperability and safety requirements are fulfilled very easily with this study. Interoperability is the ability of the subsystems to perform the events correctly and in the correct order, which ensures that the train continues its safe journey. In this study, the interoperability of the sub-systems are ensured by providing the security conditions of the systems, which is one of the most important issues. Furthermore, the complexity of the state space is reduced, so the complexity of the systems are provided more easily. In case of any error, it is easier to follow the behaviors that will eliminate the security requirements of the system, so that the CBTC system can work jointly and safely with other systems under safe operating conditions.

Lastly, the decentralized-hierarchical control architecture is built and the behavior of non-blocking and hierarchical consistency is verified. Besides, the safety requirements and interoperability are provided.

References

[1] E. Commission, "Rail Research and Shift2Rail," 2014. https://ec.europa.eu/transport/modes/rail/shift2rail_en (accessed Apr. 29, 2020).

[2] Scheidt&Bachmann, "Travis – Control Technology for Mainline Rail Traffic." https://www.scheidt-bachmann.de/en/strongsignallingstrong-systems/products-solutions/operations-control-system/control-technology-for-mainline-rail-traffic/ (accessed Apr. 29, 2020).

[3] Shift2Rail, "Shift2Rail Projects." https://projects.shift2rail.org/s2r_projects.aspx (accessed Apr. 29, 2020).

[4] P. J. Ramadge and W. M. Wonham, "Supervisory Control of a Class of Discrete Event Processes.," *SIAM J. Control Optim.*, vol. 25, no. 1, pp. 206–230, 1987, doi: 10.1137/0325013.

[5] K. Rudie and W. M. Wonham, "Think Globally, Act Locally: Decentralized Supervisory Control," *IEEE Trans. Automat. Contr.*, 1992, doi: 10.1109/9.173140.

[6] S. Jiang and R. Kumar, "Decentralized control of discrete event systems with specializations to local control and concurrent systems," *IEEE Trans. Syst. Man, Cybern. Part B Cybern.*, 2000, doi: 10.1109/3477.875442.

[7] A. E. C. Da Cunha, J. E. R. Cury, and B. H. Krogh, "An assume-guarantee reasoning for hierarchical coordination of discrete event systems," 2002, doi: 10.1109/WODES.2002.1167672.

[8] K. C. Wong and W. M. Wonham, "Hierarchical control of discrete-event systems," *Discret. Event Dyn. Syst. Theory Appl.*, 1996, doi: 10.1007/BF01797154.

[9] K. Schmidt, J. Reger, and T. Moor, "Hierarchical control for structural decentralized des," 2004, doi: 10.1016/S1474-6670(17)30759-0.

[10] K. Schmidt, T. Moor, and S. Perk, "A hierarchical architecture for nonblocking control of decentralized discrete event systems," 2005, doi: 10.1109/.2005.1467134.

[11] X. Wang, T. Tang, and S. Liu, "Study on modeling and verification of CBTC interlocking system," 2013, doi: 10.1049/cp.2013.2439.

[12] O. Kaymakci, V. G. Anik, and I. Ustoglu, "A local modular supervisory controller for a real railway

station," 2010, doi: 10.1049/cp.2010.0844.

[13] B. Malakar and B. K. Roy, "Railway fail-safe signalization and interlocking design based on automation Petri Net," 2015, doi: 10.1109/ICICES.2014.7034154.

[14] A. E. Haxthausen and J. Peleska, "Formal development and verification of a distributed railway control system," *IEEE Trans. Softw. Eng.*, 2000, doi: 10.1109/32.879808.

[15] L. H. Vu, A. E. Haxthausen, and J. Peleska, "Formal modelling and verification of interlocking systems featuring sequential release," *Sci. Comput. Program.*, 2017, doi: 10.1016/j.scico.2016.05.010.

[16] A. Fantechi, F. Flammini, and S. Gnesi, "Formal methods for railway control systems," *Int. J. Softw. Tools Technol. Transf.*, 2014, doi: 10.1007/s10009-014-0342-1.

[17] K. Kanso, F. Moller, and A. Setzer, "Automated Verification of Signalling Principles in Railway Interlocking Systems," *Electron. Notes Theor. Comput. Sci.*, 2009, doi: 10.1016/j.entcs.2009.08.015.

[18] J. Qian, J. Liu, X. Chen, and J. Sun, "Modeling and verification of zone controller: The SCADE experience in China's railway systems," 2015, doi: 10.1109/COUFLESS.2015.15.

[19] S.-H. and W. Lee Kaci C., "Structural Decentralised Control of Concurrent Discrete-event Systems," *Eur. J. Control*, vol. 8, no. 5, pp. 477–491, 2002.

[20] H. and W. Zhong W.M., "On the consistency of hierarchical supervision in discrete-event systems," *IEEE Trans. Automat. Contr.*, vol. 35, no. 10, pp. 1125–1134, 1990.

[21] RailSystem, "Communications-Based Train Control (CBTC)," 2015. http://www.railsystem.net/communications-based-train-control-cbtc (accessed Apr. 30, 2020).

[22] J. ;Sole. Farooq J., "Radio Communication for Communications-Based Train Control (CBTC): A Tutorial and Survey," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 3, pp. 1377–1402, 2017.

[23] A. Siahvashi and B. Moaveni, "Automatic Train Control Based On The Multi-agent Control Of Cooperative Systems," *J. Math. Comput. Sci.*, 2010, doi: 10.22436/jmcs.001.04.02.

[24] J. Yin, T. Tang, L. Yang, J. Xun, Y. Huang, and Z. Gao, "Research and development of automatic

train operation for railway transportation systems: A survey," *Transportation Research Part C: Emerging Technologies*. 2017, doi: 10.1016/j.trc.2017.09.009.