DOI: 10.1561/9781680838251.ch10

Chapter 10

Intelligent Transport System: The Indra Use Case

By Francisco Parrilla, Sergio Jiménez Gómez, Modris Greitans and Janis Judvaitis

10.1 Introduction

The future of the railway market involves digitization, automation, connectivity and the use of intelligent systems that continue to add value to the society by improving management, operation and user experience, in order to face the challenge posed by the European Green Deal[1] as evidenced in the different Strategic and Innovation European agendas,[2] as well as in the plans and reports of public governs and relevant public organizations and Programs (such as the Shift2Rail European Innovation Initiative,[3] the Innovation Plan for Transport and

1. https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en
2. https://errac.org/publications/strategic-rail-research-and-innovation-agenda/
3. https://shift2rail.org

Infrastructures launched by the Government of Spain,[4] the French-Swedish Strategic Partnership for innovation, green solutions in the transport sector,[5] etc).

The digitalization of the railway market, as well as the automation and deployment of new intelligent systems, requires the design and implementation of new systems to be deployed in the railway ecosystem; systems that will pose a technological challenge to achieve the objectives set in the European agendas for the coming years, and that will entail major changes as well as the deployment of a large number of devices and subsystems both On Board and On Track. These systems and devices, to face a progressive and changing digitalization of the sector, must be prepared for agile development and deployment, where their control and monitoring provide the necessary mechanisms to guarantee an efficient, robust, safe, secure and updated operation, according to the demands and challenges to be met.

The ENACT results emerges as a facilitator to meet the proposed challenge, in line with the strategic lines and programs described for the future digitalization of the rail market providing DevOps enablers.

10.2 Rationale

The rail domain requires infrastructure and resources that are usually expensive and require a long-time planning and execution. Therefore, the usage of the rail systems must be trustworthy, following strict security and safety regulations. Several functionalities could be implemented within the rail systems to ensure that the system could tackle its high critical requirements as planned.

The proposed Use Case for railways shows how the use of the ENACT enablers can be used to enhance the DevOps cycle of new innovative systems – aligned with other innovation programs mentioned in the Chapter 10.1 – exploiting and evaluating their potential. The selected innovative systems have been analyzed, implemented and tested:

- **On Board WTI (Wireless Train Integrity)**[6]: This functionality is in charge of measuring, in real time, train composition parameters and evaluate them

4. Ministerio de Transportes, Movilidad y Agenda Urbana. Gobierno de España: "Plan de Innovación para el Transporte y las Infraestructuras". February 2018

5. https://www.tresor.economie.gouv.fr/Articles/2018/03/28/partenariat-franco-suedois-pour-l-innovation-et-les-solutions-vertes-french-swedish-partnership-for-innovation-and-green-solutions

6. Aligned with On Board Train Integrity Technology demonstrator tasks defined on TD2.5 addressed on X2RAIL-2 and X2RAIL-4 projects on which Indra is involved https://projects.shift2rail.org/s2r_ip_TD_D.aspx?ip=2&td=061d0fcf-51a6-4358-a74f-a4d34e8dac01 and making use of SCOTT https://scottproject.eu/ and DEWI results http://www.dewiproject.eu/

to report the train integrity status. The On Board system, based on WSN Sensors among the composition, provides the necessary information to determine the rolling stock material that composes the consists and evaluate and ensure, through an On Board unit, its integrity status. This integrity status is shown to the driver through the Train Management Systems (TMS) and a Cloud service interface.

- **Logistic and Maintenance System**[7]: This functionality provides information to register and locate both rolling stock material and on-track signalling devices and inform about their status. This functionality is required to solve the rail environment needs to locate and monitor the status of the big heterogeneity and flexibility of the compositions and signalling devices, making a special emphasis on the freight compositions, to optimize the rail business operation. The points that are optimized into the rail framework are the management of the rolling stock, cargo tracking, etc. To this end, it is required deploying IoT On Board and On Track, together with Cloud solutions to track and manage the rolling stock material data and to perform predictive maintenance.

These services are illustrated in the following Figure 10.1:

The DevOps role in the Use Case assists to reach this automation and digitalization objective, with the following focuses:

- **Security and Privacy Monitoring (S&P Mon&Con) tool**: This tool is responsible for monitoring and actuating over the On Board infrastructure to guarantee its security characteristics.
- **GeneSIS tool**: This tool monitor performs software remote deployments on the rail equipment to keep all the devices with the desired software version.
- **Behaviour Drift Analysis (BDA) tool**: This tool monitors the behaviour of the equipment to detect deviations related with the proper define behaviour for them.
- **Actuation Conflict Management (ACM) tool**: This tool detects conflicts that may appear in the Use Case operation and to help to resolve the conflicting actions.
- **Testing and Simulation tool**: It is a tool that simulates a part of the Use Case infrastructure and makes a Digital twin of it to be evaluated.

7. Aligned with Smart radio-connected all-in-all wayside objects demonstrator tasks defined on TD2.10 addressed on X2RAIL-1 and X2RAIL-4 projects on which Indra is involved https://projects.shift2rail.org/s2r_ip_TD_D.aspx?ip=2&td=061d0fcf-51a6-4358-a74f-a4d34e8dac01 and making use of SCOTT https://scottproject.eu/ and DEWI results http://www.dewiproject.eu/

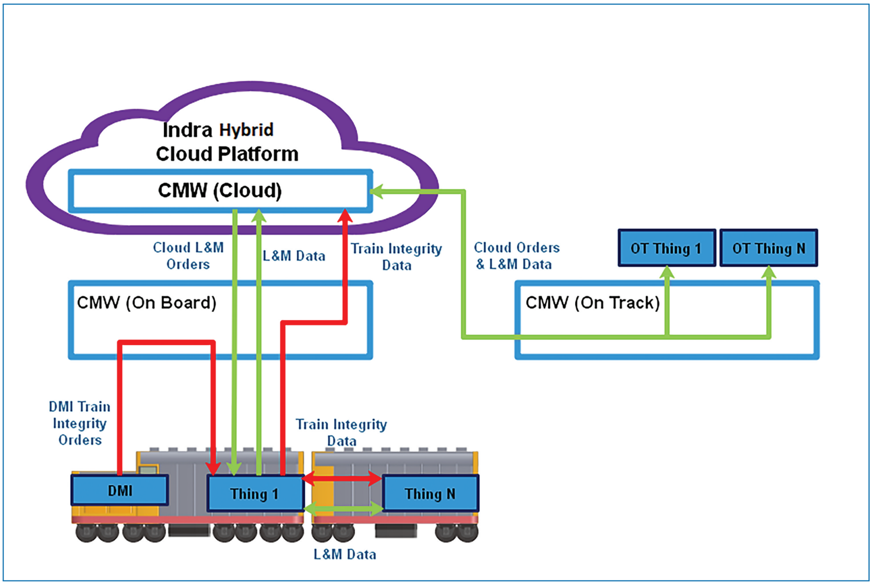

Figure 10.1. On Board WTI (Wireless Train Integrity & Logistic and Maintenance System Functionalities Scheme).
Source: INDRA.

- **Root Cause Analysis (RCA) tool**: This tool detects possible failures that may occur in the Use Case infrastructure informing about the most likely cause for that fail.

One of the challenges that the Use Case faces to reach the automation and digitalization of the rail environment is the scalability. The mentioned DevOps tools developed in ENACT for the Use Case have different objectives. However, these objectives converge on solving the scalability issues that the functionalities hide. To evaluate the scalability impact and to provide the issue's magnitude, a real rail scenario example is provided. An example to show the scalability issues is the Madrid-Barcelona French Border line, one of the first high speed lines built in Spain and one with the higher capacity (more trains per day). An example of a real line magnitude can be seen in Figure 10.2.

For this real example, focusing only on On Board systems, there are 94 trips circulating through this line: 47 of them from Madrid to Barcelona and the rest from Barcelona to Madrid. Each trip is accomplished by a single train composition that could be built following three different kinds of composition: simple, double, and mixed.

- **Simple**: There are 38 simple train compositions per day where there is only one locomotive wagon. Each simple composition is formed by 12 wagons.

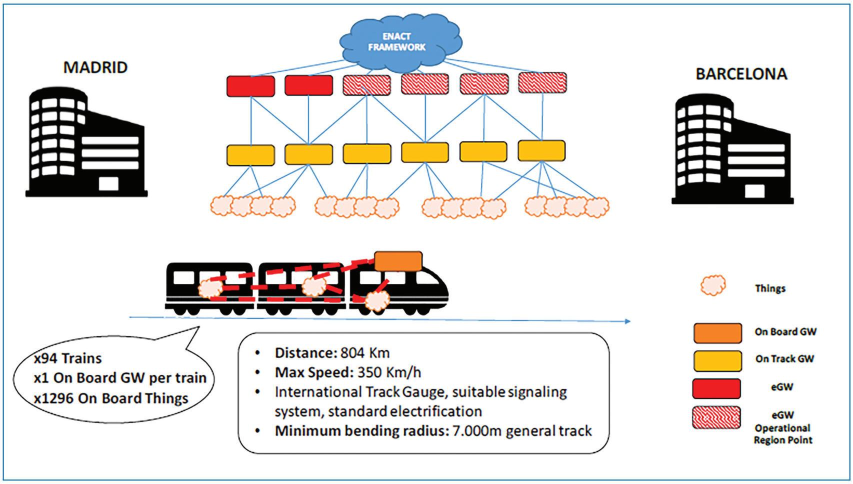

Figure 10.2. Madrid-Barcelona French Border rail line general characteristics. *Source*: INDRA.

- **Double**: There are 5 double compositions per day where there are two simple compositions joined. Each double composition is formed by 24 wagons.
- **Mixed**: There are 5 mixed compositions per day which are formed by different kind of pieces of rolling stock. Each mixed train composition is formed by an average of 18 wagons.

In the real line, there are running 1296 wagons in average, if both directions of the line are considered (94 trains per day). Based on the functionalities architecture, further details shown in Section 10.3, it is estimated that around 4000 units of On Board equipment are required to cover the On Board equipment for this line.

From the magnitude presented, we can verify that it is essential to provide a deployment mechanism to update all these systems in a controlled, automated and orchestrated way. It is important to remark that these systems should be developed with digital twins in mind to test the potential impact of new updates in a test environment. They faithfully reproduce the potential impacts of these updates in operating environment with mechanisms that ensure the cybersecurity of communications throughout the ecosystem and adjusts the deviations of the sensor networks involved. This serves to ensure the robustness of the different orders distributed throughout the global system.

10.3 Use Case Implementation

In this section, we explain the IoT platform brought to implement the rail functionalities and show how the ENACT enablers are applied. Moreover, it includes how

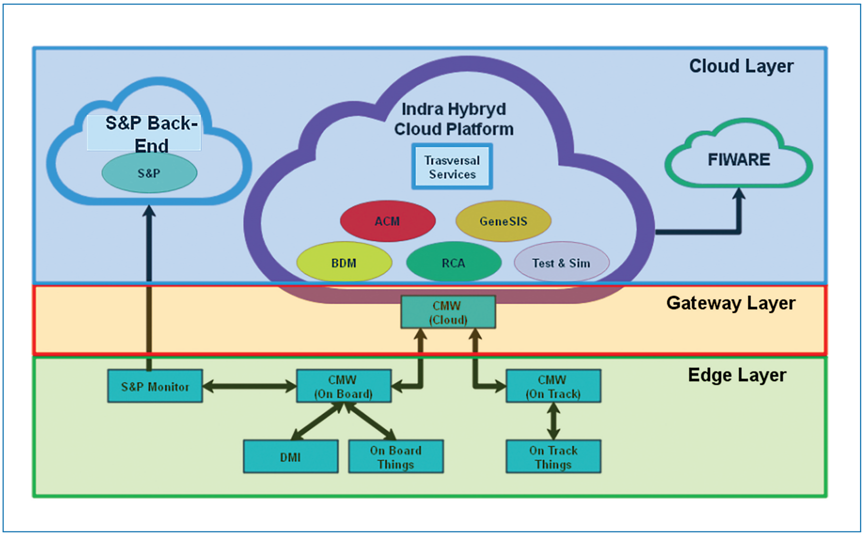

Figure 10.3. Rail Use Case architecture enriched with the DevOps tools. *Source*: INDRA.

the DevOps tools enhance the Use Case itself. As illustrated in the Figure 10.3, we identify three different architecture layers. These layers are the Edge, the Gateway, and the Cloud layers:

10.3.1 Edge

The edge layer is made up of the various objects (Wireless Sensor and actuator networks – WSAN – and other concentrating and/or communication devices) distributed both on the track and in the On Board equipment. This layer also serves to provide/send raw data to the functionalities. It is used by the BDA (10.4.5) and ACM (10.4.4) tools to perform conflict analysis and monitor the behavior of the devices Moreover, it is used by the Testing and Simulation tool to create a fair Things Digital Twin. The following elements form it:

- **Things**: The key element in this layer is defined under the name of Thing. The Things provide the functionality parameters described above.
  The Things are defined as a group of nodes which globes coordinators, sensors or actuators. In such a way, the Things have several capabilities: gather, actuate and communicate.
  It must be emphasized that the layer covers the On Board and On Track sections. WTI and a set to Logistic and Maintenance parameters are obtained and processed in the On Board section, while the On Track section participates in the provision of another set of Logistics and Maintenance

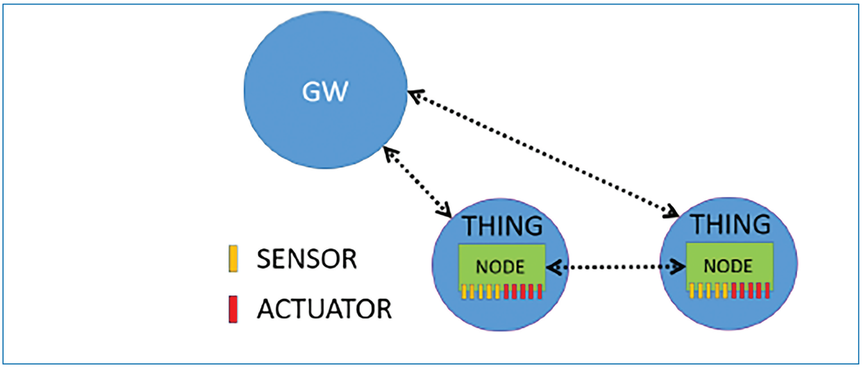

Figure 10.4. On Board and On Track Things.

Source: INDRA.

specific data. The On Track infrastructure uses RFID technology to obtain information from the train. These Things are powered up by an energy harvesting system to cover the case that no electrification systems are equipped On Board a train.

– Sensors:
  - On Board: an accelerometer, a Received Signal Strength Indicator (RSSI) sensor, and a Global Navigation Satellite System (GNSS) receiver, and Radio Frequency Identification (RFID) tag and reader.
  - On Track: RFID reader.

– Actuators:
  - On Board: Light-Emitting Diode (LED)s and displays.

The Things software consists of 5 modules: data managing module, inauguration module, integrity module, logistics module and maintenance module. They are working in synergy to provide the data and control over the On Board and On Track Things infrastructure deployed on the rolling stock.

– Data managing module:
  - *On Board*: The data is gathered at the nodes located on each wagon of the train. Data are sent over the air using the IEEE 802.15.4 based ZigBee protocol for secure and reliable communications. As typical for wireless sensor and actuator network, there is at least one so called base station, which forwards the data to the next processing point. The system is also capable of communication in the other direction sending commands from base station to the nodes.

    In this case the next processing point is WSN coordinator. WSN coordinator acts as a data forwarder from Things to the Communication middleware (CMW), while also ensuring that the data forwarded are in the correct format. WSN coordinator is also responsible about the forwarding of commands to the Things from CMW. The commands from CMW can be: start inauguration, start/stop integrity control, start/stop logistics control, start/stop maintenance control and reset. All of the commands are part of modules described in next sections.

- *On-Track*: The on-track data gathering does not require the wireless network, the RFID sensor readings are gathered and forwarded to the CMW. On-track infrastructure listens to the following commands from CMW: start/stop logistics control and reset.

– Inauguration module: The inauguration module is implemented on the WSN coordinator. After receiving the command about the start of inauguration procedure from the CMW, the base station is notified to identify the nodes located on the wagons belonging to this train and check that they are operational. In this module also the physical order of the wagons is calculated using the GNSS and RSSI sensor values and RFID data. After successful inauguration the WSN coordinator sends corresponding message to CMW reporting the inauguration status.

– Integrity module: The integrity module is operated only in the On Board infrastructure and is responsible for continuously validating the train integrity while it is operational. Integrity control can only be started after a successful inauguration phase is finished and integrity control is not already operational. When the WSN coordinator receives the command from CMW to start the integrity control it notifies the base station to send out the integrity start command. After start command each of the nodes and base station reports sensor status every 250 ms or 4 times per second. The received sensor data is forwarded to the CMW as raw data consisting of GNSS position, accelerometer data and RSSI value measured at the base station for each wagon. Using this information also the train integrity is calculated, it is based on aforementioned sensors and train integrity is considered lost in case when at least two of three sensors report data that indicates that there is a train integrity issue. The train integrity information is also forwarded to the CMW. The train integrity system remains operational until the stop or reset command is received. If the start inauguration or start integrity command is received while the integrity system is operational, the command is ignored.

– Logistics module: The logistics module is responsible for providing the business information about the train logistics. Logistics module operates on the On Board and on-track infrastructure and uses the RFID reader data. On-track infrastructure provides wagon order information, but On

Board infrastructure provides information about the cargo and also allows to identify the wagon by RFID tag associated with it. The logistics module can be started after successful inauguration and stopped at will.

- Maintenance module: The maintenance module is responsible for providing the maintenance information about the wagons and infrastructure. While the maintenance module is operational it reports the node energy consumption and battery charge status. The maintenance module can be started after successful inauguration and stopped at will. Also the maintenance module handles the reset command, which can be issued by CMW and will reset the Things software in case of any errors. The reset command will not be accepted by the WSN coordinator if inauguration process is running or integrity control module is operational.
- Testing and validation: The developed infrastructure was validated using the demo setup of Lego train with minimal changes to the setup described above due to physical limitations of Lego train. The demo setup with Lego train was used to provide the partners with sensor, logistics and maintenance data from the on-track and On Board infrastructure while located in the lab environment but still providing non-generated data, thus making it easier to test, integrate, debug, and showcase developed technologies.

• **DMI**: The DMI (Driver Machine Interface) is included into this layer and it is responsible for managing the Things into the train by the driver and to perform Safety data treatment for the functionalities.

• **S&P Monitor**: This equipment is the key element in the security properties for the Use Case Edge layer. The S&P Monitor is an architecture component located On Board in charge of monitoring the traffic that is carried by the gateway layer 10.3.2. It must be emphasized that the traffic analysis ignores the business data related with the ITS functionalities. The reason behind this decision is that the functionality is in charge of covering the security aspects of the On Board equipment out of functionality focus. This elements is formed by several differentiated entities:

  - Hardware: The hardware offers the computing capacity to the software, the connectivity with the gateway by Ethernet and the connectivity with the S&P Mon&Con Back-end through a 3G/4G interface.
  - Monitor SW: The monitor software sniffs the traffic from the gateway in order to be treated and to be sent to the S&P Mon&Con Back-end for a further analysis.
  - User's removal Software: The S&P Mon&Con Back-end analysis could throw as a result that the users that generates the traffic monitored are intruders, therefore, a notification with the users is published to this

entity. This entity, developed by Indra, revokes the user in the ITS central authentication services.

10.3.2 Gateway

The gateway, so called CMW (Communication Middleware), is the element that connects all the Use Case system elements. It gathers the edge data and provides it to the Cloud. Moreover, it gathers the orders to the Things to start the functionality services. This CMW is based on Indra developed solution certified for rail environments.

From a general perspective, the basic functionalities of this CMW are as follows:

- Routing the messages from the different services to be sent to the different architecture entities. This routing follows a preconfigured topology to guarantee the provision of the information in a safe and secured manner.
- Synchronization tasks to keeps all the devices working with the same time reference.
- Authentication tasks at different OSI levels to enable the connectivity of the edge elements and to enable the connection of the CMW with the Cloud layer.
- Provision of CMW status metadata to be evaluated by the DevOps tools.

The Use Case, into the ENACT project framework, relays part the scalability issues to the CMW. As the CMW equipment cost is high to provide several of these devices to the project, considering the budget, the scalability is tests will be done in a single physical CMW and several virtual ones will be provided for testing. Therefore, the general architecture is formed by a single physical CMW located On Board and the several virtual CMWs.

10.3.3 Cloud

The Cloud layer is formed by the Cloud platforms that participate on the Use Case and how they are related. Three different Cloud platforms are considered: FIWARE [1], Indra Hybrid Cloud Platform, and S&P Back-end.

- **Indra Hybrid Cloud Platform**[8]: The cloud is a hybrid solution that combines a private and public part. The private par is in charge of the internal

8. https://www.igi-global.com/chapter/security-in-rail-iot-systems/258896

ITS task such as edge data storage, edge elements authentication, and external partner's authentication. The public part is in charge of integrating external elements such as tools or other Cloud platforms. This is the integration point made for all the Cloud resources and DevOps tools that require it. All the DevOps tool, except the S&P tool, are integrated in this layer to accomplish their functions. Moreover, it is the integration point also for the FIWARE Cloud platform.

- **FIWARE**: FIWARE is an open source platform that the European Union supports as a future platform to provide Cloud services. For this Use Case, the FIWARE tool can allocate several functionalities that goes from systems authentication, storage, DevOps tools integration. However, for the ENACT project the functionalities uses this Cloud platform to provide to the Use Case user several dashboard to track the Use Case functionalities (making use of the FIWARE ORION component for integration tasks and FIWARE Grafana component as the presentation tool).
- **S&P Mon&Con Back-end**: It is a service in a separate Cloud that supports the security monitoring capabilities. The traffic and security data treated in the S&P Monitoring tool is sent to this back-end to be evaluated. The service provides to the Use Case user with an interface to interact with the traffic behaviour and security rules that are desired for the On Board installation, as well as it offers the situational awareness functionalities for the user to get informed on the security status at all times.

10.4 DevOps of ITS System Powered by ENACT Tools

This section is intended to introduce the specific functionalities that the DevOps tools use and how these has been implemented and tested to enhance the Use Case itself.

10.4.1 Security Monitoring (S&P Mon&Con)

The Security and Privacy Monitoring and Control Enabler (for short, S&P Mon&Con) is in charge of providing the security layer that it is required for the Edge, as IoT technologies can suffer multiple types of attacks at this layer. The monitoring service of the tool is the one used in the Use Case. The S&P Mon&Con is the only tool that it not integrated into the Use Case at the Indra Hybrid Cloud Platform, as it acts as supervisor of the Use Case IoT system checking from outside whether resources at the Edge could be under compromise, thus, it has a parallel

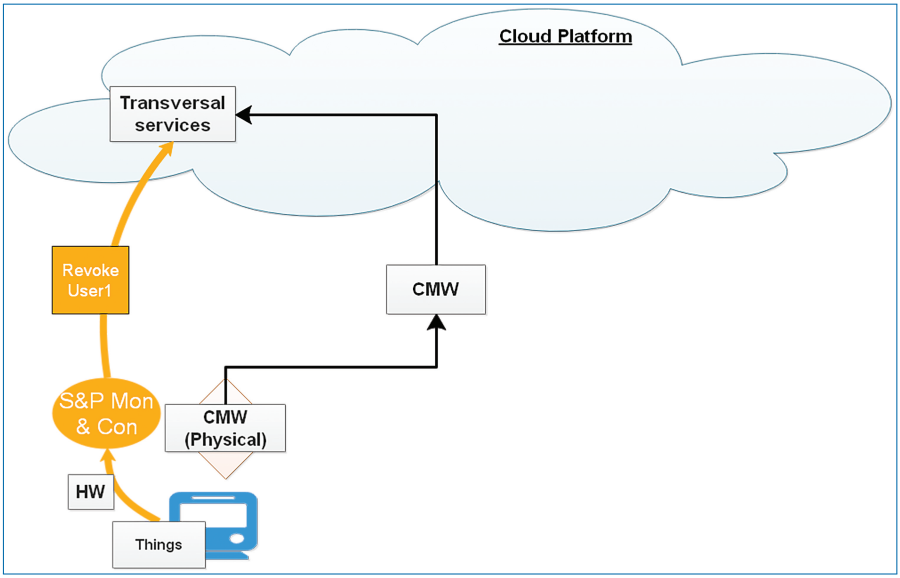

Figure 10.5. S&P – Rail Use Case integration synoptic.
Source: INDRA.

deployment and a different integration philosophy. A synoptic of the scenario can be seen in the Figure 10.5.

The tool is divided into two sections, the monitoring and the actuation part. The monitoring part is in charge of collecting the data that are going through the On Board gateways, this data includes the Things and the DMI data only. These data is monitored and sent throw a specific On Board device to the S&P Monitoring Back-end to be analysed. From this analysis the following parameters are analysed:

- **Traffic behaviour monitoring**: The traffic behaviour is considered as one of the characteristics that defines the rail functionalities is regular. The Safety and Security requirements that defines this kind of functionalities require a regular traffic that may be affected by intruders. The S&P tool is focus on detecting deviations in this edge layer traffic and revoking the user, from the Use Case central authentication servers, that generates that deviations.
- **Intrusion detection**: The authorised users are those systems that can publish/subscribe to IoT Platform (authenticated in the central Use Case authentication server), and are registered in the S&P Monitoring tool registry (both user id and Media Access Control (MAC) addresses). In case a user is authenticated in the central Use Case authentication server but not in the S&P Monitoring tool database, that user or/and the device they use will be revoked

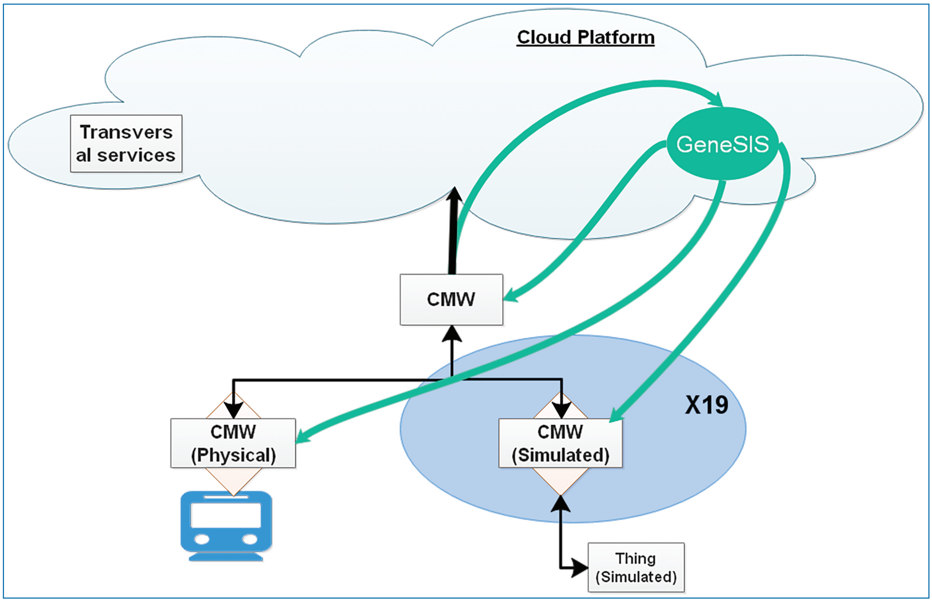

Figure 10.6. GeneSIS – Rail Use Case integration synoptic.
Source: INDRA.

in the Use Case central authentication servers, banning its connectivity to the whole IoT Platform.

10.4.2 Automatic Deployment – GeneSIS

The tool is in charge of managing and controlling the software that is running in the ITS Use Case.

It deploys the Docker images running in the gateways and ensures that they are correct and deployed with the access credentials requires to be integrated into the ITS infrastructure. A synoptic of the scenario can be seen in the Figure 10.6.

The tool also is aware of the status of the system deployed. The tool monitors the status of the Use Case infrastructure to check if it is possible making a deployment or not. In case the system is running the Use Case functionalities, the deployment cannot be performed. Moreover, the tool is able to evaluate if the deployment is correctly performed and if it has a conflict with previous deployments made in the same device.

10.4.3 Testing and Simulation

The testing and simulation tools has two roles into the ITS Use Case. The first one is monitoring the infrastructure in order to validate that the ITS infrastructure

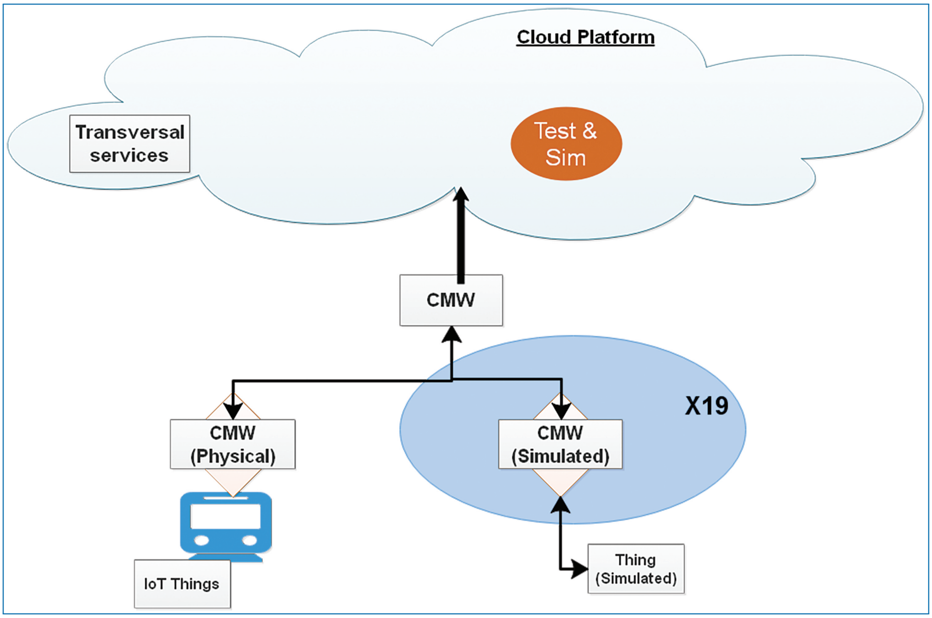

Figure 10.7. Testing and Simulation – Rail Use Case integration synoptic.
Source: INDRA.

is running properly and to simulate failures into the infrastructure to enhance the validation value against issues that may appear into the operation of the Use Case itself. A synoptic of the scenario can be seen in the Figure 10.7.

The Testing and Simulation tool collects all the data gathered by the gateway layer to monitor its workload when it is operating the rail functionalities' tasks. In this case, all the traffic from the Edge and Cloud layers is monitored, in other words, the 100% of the traffic managed during an operation by the gateway.

Using these data the tool is able to replicate a single gateway, in a simulated virtual environment, taking as a basis the behaviour of the monitored gateway. This procedure that replicates the devices in a virtual infrastructure is called Digital Twin. Generating several Digital Twins as many times as desired provides the tool's user the possibility to generate a virtual scenario with all the gateways desired; hence, the scalability of a scenario can be proved. Moreover, as the virtual infrastructure is generated, the tool is able to simulate certain situations that may compromise the infrastructure and check its reliability.

This simulated environment is not enough to test the system's scalability. Several metrics to evaluate the simulated gateways are required. A specific report about the gateways status is required to know how the gateway is dealing with that monitored data. As it is mentioned in the Section 10.3.2, the gateways report specific data about its physical and routing status to evaluate their operation. Therefore, the tool is able to infer, using these reports, the behavior of this simulated infrastructure in any situation proved.

10.4.4 Actuation Conflict Management (ACM)

The ACM tool is intended to manage conflicts that may appear in the train operation. This tool is based on generating behavioural models that can be applied to the On Board devices to fix an specific behaviour depending on the rail system inputs. A synoptic of the scenario can be seen in the Figure 10.8.

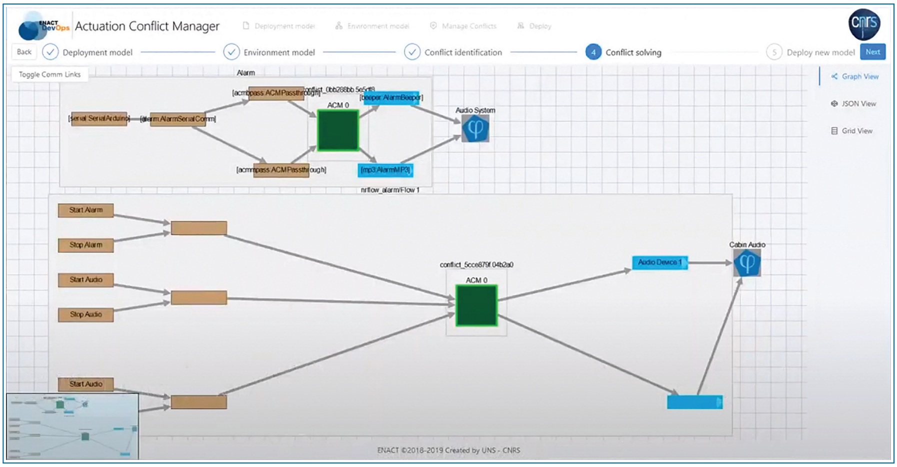

Figure 10.8. ACM – Rail Use Case integration synoptic.
Source: INDRA.

Based on the operation iterations, the developer can check the conflicts that may appear. The Safety and Secure functionalities defined are designed to not generate conflicts in the operation; however, the non-Safety systems that uses the safety ones may generate conflicts between their behaviours (e.g., audio announcements, alarms, etc.).

The ACM tool is able to generate models, as shown in the Figure 10.8, which can be deployed in any device that is the root cause of the conflict.

10.4.5 Behavioral Drift Analysis (BDA)

The BDA in charge of checking that the Things behaviour matches with the real modelled behaviour defined for them. The tool monitors the business data published by the Things to the Cloud layer to check in real time deviations with the mentioned model.

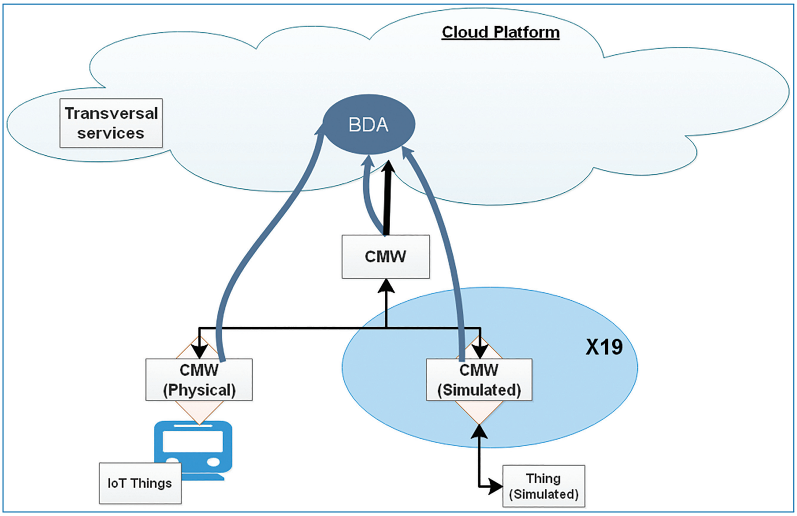

Figure 10.9. BDA – Rail Use Case integration synoptic.
Source: INDRA.

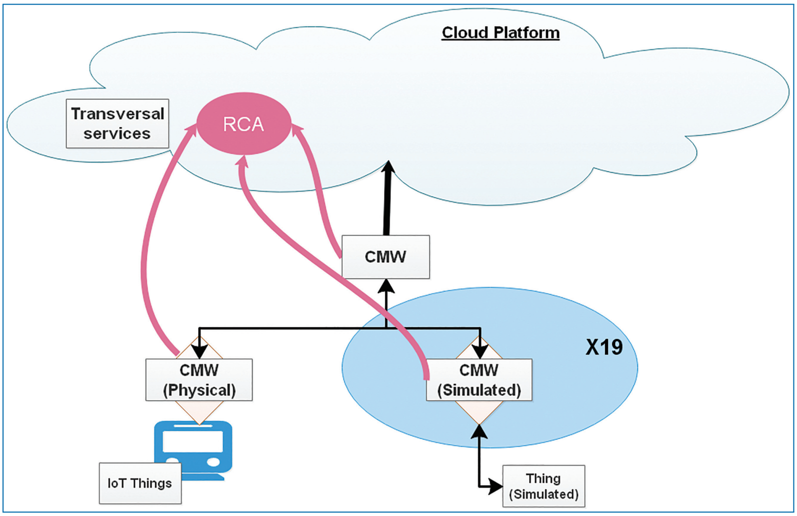

Figure 10.10. RCA – Rail Use Case integration synoptic.
Source: INDRA.

10.4.6 Root Cause Analysis (RCA)

The RCA tool is in charge of checking the security perspective of the ITS infrastructure from the gateway to the cloud layer finding the reasons for a failure that may occur (Figure 10.10). This tool serves to identify the cause of network mistakes that in a scalable systems is critical due to the quantity of devices deployed.

Several failure scenarios are simulated and recorded by the RCA tool in order to store the behaviour of the infrastructure in case of those failures appear. The data monitored is the physical and routing data reported by the gateways.

10.5 Conclusion

We have tested and validated – focused on developing trustworthy and ready-to-use scenarios to test the DevOps Enablers – the ENACT DevOps framework. From the Use Case perspective, the provision of an IoT platform with the characteristics exposed along the chapter makes a first step to enhance the rail environment and improves the new systems for the future digitalization and automation to an industry that is experiencing a huge evolution in the last decades.

The main impacts that the DevOps philosophy have on the rail environment, based on the mentioned DevOps tools that are listed along the document, are focus on:

- Ensuring the scalability of the system before deploying it. Introducing a Testing and Simulation tool permits the optimization of the infrastructure components and reduces the uncertainty about the system reliability. Therefore, the on-site testing time is reduced.
- Fast and agile deployment of new software versions in a remote manner, this reduces the infrastructure functionalities updated and the maintenance costs.
- Provision of a security backup to the internal rail authentication mechanisms covering since the devices to the application layers. The S&P tool locates the system intruders in a more accurate manner and the by design rail Security and Safety aspects are increased.
- Monitor the deviation in the behaviour of this systems in real time during the operation. The BDA tool helps to locate devices issues in a more accurate manner and, then, as the diagnosis time is improved the maintenance time and tasks is reduced.
- Ensure the interaction between the drivers and the rail functionalities to reduce the human errors. The main impact is the reduction of the failures that may occur in the system caused by the driver. This is highly relevant as the driver is a key factor to rely on the security and safety aspects in the rail environment.

Reference

[1] Indra Sistemas S.A. Contribution. *X2Rail-1 Deliverable D7.2 – Railway requirements and Standards application conditions – Indra Sistemas S.A Contribution*. Tech. rep. May 2018.