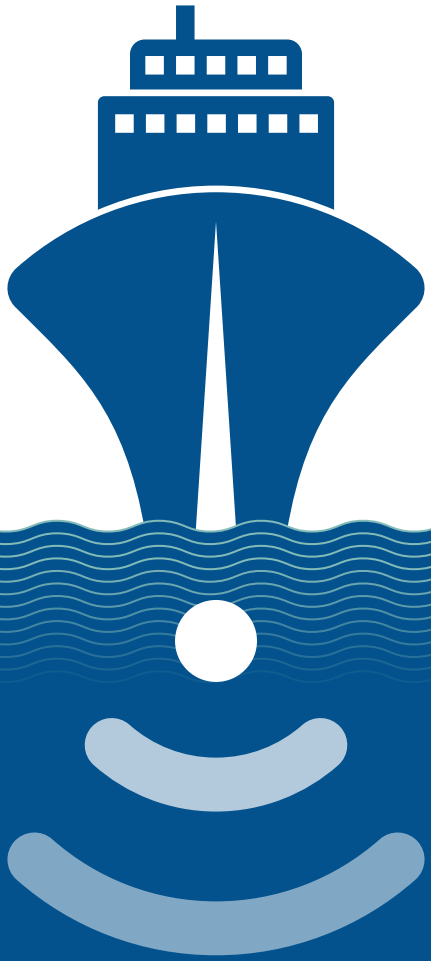
GSMA Internet of Things

SECURING THE PORT OF THE FUTURE

SECURE IoT SOLUTIONS FOR THE SMART CITY



www.gsma.com/IoTSecurity

SECURING THE PORT OF THE FUTURE

SUMMARY

LED BY THE UNIVERSITY OF SEVILLE AND THE PORT AUTHORITY OF SEVILLE, THE TECNOPORT 2025 PROJECT USES INTERNET OF THINGS (IoT) SOLUTIONS TO IMPROVE THE EFFICIENCY OF TRANSPORT AND LOGISTICS IN SOUTH WEST SPAIN.

Implemented by a consortium of five companies, including telecoms operator Telefónica, the project uses new wireless networks and sensors to improve the tracking and remote control of containers passing through the port, and to optimise the rail and river traffic in the area.

Led by the University of Seville and the Port Authority of Seville, the Tecnoport 2025 project uses Internet of Things (IoT) solutions to improve the efficiency of transport and logistics in south west Spain. Implemented by a consortium of five companies, including telecoms operator Telefónica, the project uses new wireless networks and sensors to improve the tracking and remote control of containers passing through the port, and to optimise the rail and river traffic in the area.

In line with the GSMA IoT Security Guidelines, Tecnoport 2025 uses a combination of virtual private networks (VPNs), private access point names (APNs), multiple-factor authentication mechanisms and other measures to keep the new IoT solutions secure. In the fourth quarter of 2016, Tecnoport 2025 employed the new GSMA IoT Security Assessment scheme to test the security of two key components of the project – the managed connectivity platform that controls cellular connectivity, and the FIWARE-based Smart City Platform that aggregates the data generated by remotely deployed sensors connected via wireless networks. As well as ensuring these components are secure, the assessment scheme is helping Telefónica to refine its IoT security proposition and the other members of the Seville consortium to further strengthen the security of their networks and systems.

TURNING SEVILLE INTO A SMART PORT

The Port of Seville on the Guadalquivir River is an important logistics hub that serves an area that is home to more than one million people. The port is also on a major trade route between Madrid and the Canary Islands. In July 2014, the Port Authority of Seville launched the Tecnoport 2025 project to improve the efficiency of its operations by harnessing information and communications technologies (ICT).

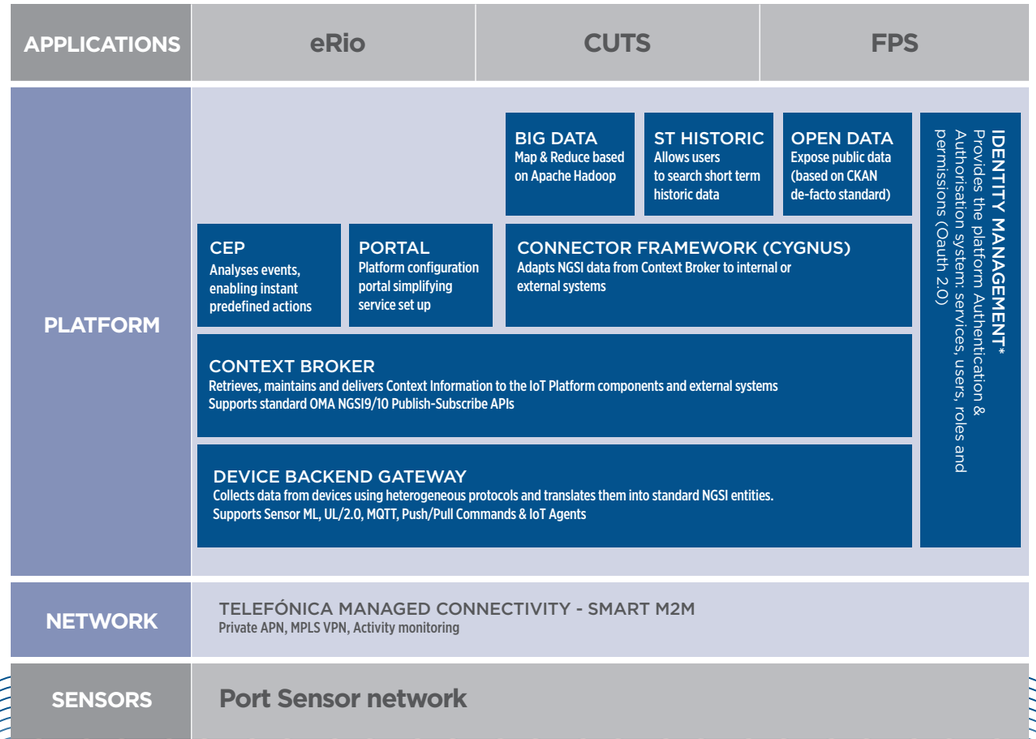
Led by the University of Seville and part-funded by the EU, the €7 million IoT project was implemented by a consortium of five companies - Telefónica, Thales Spain, Isotrol, Portel and Serviport.

The project has three key work streams:

- To improve the tracking and remote control of containers passing through the port;
- Optimisation of rail traffic in the vicinity of the port;
- Optimisation of traffic on the Guadalquivir River.

Antonio Torralba, a senior professor at Seville University and principal engineer at Tecnoport 2025, believes the ICT architecture developed for the project (shown in the graphic below) will help define a framework for the smart port of the future.

TECNOPORT 2025



SECURITY BY DESIGN

Each of the three solutions developed for tecnoport 2025 was designed to be secure from the outset. Jose Rodriguez Perez, who leads the IoT security activities at Telefónica, and his colleagues employed the GSMA IoT Security Guidelines to ensure that the new solutions followed best practice in terms of security. For example, Telefónica's managed connectivity platform is able to detect anomalies on connected devices and control their data usage, as recommended in the GSMA guidelines. The consortium also maintains a clear separation of data between users, employs secure keys, and requires users to authenticate themselves with multiple factors.

As the Tecnoport 2025 solutions use a combination of intrinsically secure cellular networks and wireless networks operating in unlicensed spectrum, Telefónica employs a combination of private access point names (APNs) and virtual private networks (VPNs) to connect the remote sensors to the Smart City Platform. Although it can be difficult to secure non-cellular connectivity, Jose Rodriguez Perez says the "private APNs and VPNs can provide a very high level of security." Access to the various communications networks is also controlled by SIM cards and other mobile authentication solutions.

ABOUT THE GSMA IoT SECURITY GUIDELINES AND ASSESSMENT

In February 2016, the GSMA published the IoT Security Guidelines, a set of best practices for the secure end-to-end design, development and deployment of IoT solutions on any mobile network. Based on the expertise and collective knowledge of the mobile telecommunications industry, the guidelines offer valuable insights and recommendations to enable the creation of trusted, reliable and scalable IoT services.

The new GSMA IoT Security Assessment scheme enables IoT companies to demonstrate that their products are aligned with the GSMA guidelines. By submitting an assessment, IoT companies can demonstrate the security measures they have taken to protect their products and services from cyber security risk, enhancing their reputation as trusted IoT service providers.

The GSMA IoT Security Assessment scheme covers security controls for the whole ecosystem and further enhances the alignment of all stakeholders by putting in place a concise framework with consistent terminology and a structured approach to IoT security information. It enables companies to check whether their security measures align with the best practice outlined in the GSMA IoT Security Guidelines. Companies can use the assessment to address weaknesses in their products and services, and demonstrate to their customers that they are taking cyber security seriously.

ASSESSING THE EFFECTIVENESS OF THE SECURITY MEASURES

Soon after the GSMA published the GSMA IoT Security Assessment scheme (see box) in the autumn of 2016, Telefónica used the tool to evaluate the security of two key elements of the Tecnoport 2025 architecture: the managed connectivity platform and the FIWARE-based Smart City Platform, which collects the data captured by the wireless networks.

"We chose to do the assessment component-by-component because it is then valid for many other customers," says Jose Rodriguez Perez. "We can reuse the results, which can be a benchmark for other projects, such as the smart city solution we have deployed in Valencia."

Following the assessment, Telefónica has introduced some further controls on the network monitoring side of the solution. "The process has been useful for us," says Jose Rodriguez Perez. "As a result of the assessment, there have been inputs to the roadmap: some ideas for new products. In our smart m2m solution, we have included some monitoring controls. We can blacklist or disable devices if they are in a strange location or if they are consuming too much data. We also have some ideas about using machine learning to create new algorithms and improve partner detection information and we are working on them with Eleven Paths, the Telefónica security company."

Although the assessment process is straightforward, it can provide a wealth of useful information that can be used to strengthen security further. "It takes time to perform it properly, as the recommendations are very complete," Jose Rodriguez Perez says. "You use a checklist, which is very useful for highlighting what needs to be done and ensuring you conduct the assessment properly."

“The new solutions have increased the competitiveness and efficiency of the port, which is very interested in innovation,” concludes Antonio Torralba. “And the security is a critical part of the solution.”

NEXT STEPS

Telefónica plans to present the results of its IoT security assessment to the other members of the consortium, as well as other customers, and to encourage them to conduct a similar exercise. We have found it to be a very powerful way to exchange information,” says Jose Rodriguez Perez. “If we all use the same assessment tools, it will ensure we are speaking the same language as customers. If you assess your infrastructure with your own language and then share that information with others, there can be misunderstandings.”

Telefónica has found that the assessment process has helped to highlight some important security features that its partners in the consortium need to be aware of. For example, the Tecnoport 2025 team has now enabled some security features on the remote sensors that hadn’t been considered before. Moreover, the process has underlined the importance of using controls for access to the private APNs and isolating connected devices from the Internet. Such measures help to ensure that connected devices can’t be hijacked by malicious bots. In a high-profile case in October 2016, hackers used Wi-Fi connected consumer appliances, protected only by default usernames and passwords, installed in homes in many different markets to perform denial of service attacks on leading web sites.

Antonio Torralba of Seville University says his team is in close contact with Telefónica on security and has implemented all the security aspects that the operator has recommended. He adds there are plans to use a similar approach, together with the FIWARE data aggregation platform, as the basis of other smart city services in the port and the city of Seville. “The Port of Seville is thinking of extending the coverage of this platform to include some administrative information,” he says. More broadly, the consortium is now using the FPS system (see box), developed to optimise the use of the rail network, as the basis of a new product for the rail sector.

“The new solutions have increased the competitiveness and efficiency of the port, which is very interested in innovation,” concludes Antonio Torralba. “And the security is a critical part of the solution.”

HOW TECNOPORT 2025 IS OPTIMISING LOGISTICS IN SOUTH WEST SPAIN

The Tecnoport 2025 project employs a multi-protocol communication network, and a platform for service integration based on the FIWARE standard. “The development work started in July 2014 and ran for 18 months, which is a very tight schedule for a project with this level of ambition,” says Antonio Torralba, a senior professor at Seville University and principal engineer at Tecnoport 2025. “We needed a public-private partnership with a combination of capabilities to complete the project in the required timeframe.”

The consortium developed the Cooperative Unitized Tracking System (CUTS) to enable the location of containers to be tracked in near real-time and to enable remote control over the containers’ refrigeration systems. Telefónica deployed a wireless network (using the 802.15.4g protocol) in the port facilities, warehouses and to cover the various transportation modes (ships, trucks and trains). This network employs wireless concentrators to collect data from terminals attached to the containers as they pass through the coverage area of the concentrator. The concentrators communicate with the central server via the cellular network or a satellite terminal. Using several layers of routers, these wireless sensor networks can be configured to stretch to 10 kilometres and can support up to 5,000 terminals per network. The solution aims for a maximum latency time of 20 minutes.

The demo phase, conducted in the last quarter of 2015, connected 50 containers, three trains, five trucks and three ships. The data concentrators were deployed in one warehouse and one dry port in Madrid, in the transport infrastructure, in the Port of Seville and in two container terminals in the Canary Islands. The demo phase demonstrated the functionality of each sub-system and their integration into the overall CUTS solution.

To optimise rail traffic in the vicinity of the port, the consortium developed the Ferro Port System (FPS) system, which allows real-time monitoring of trains’ position, length and speed. It also automates switching points, level crossings, signalling and other elements of the rail infrastructure, while providing train drivers and operators with far more detailed real-time information than they had in the past.

The third strand of the Tecnoport 2025 project saw the introduction of the e-River Information and Optimization (EIRO) system to manage traffic on the Guadalquivir River. As well as being used by leisure traffic, this waterway is an important trade route. However, its navigability is limited by the shallow waters, which make it greatly dependent on the tides. The EIRO system uses the IEEE 802.15.4g protocol, and several layers of routers, to create wireless networks stretching over 20 kilometres. As well as monitoring the positions of vessels on the river, the solution monitors hydrological and meteorological conditions, waterway conditions, water quality and spillage. The EIRO system can also be used to send commands to the equipment deployed along the river. The information collected by the EIRO system is used to inform a traffic scheduler, which takes into account the composition of convoys entering and leaving the port, and the waterway conditions.

ABOUT GSMA INTERNET OF THINGS

THE GSMA'S INTERNET OF THINGS PROGRAMME FOCUSES ON ENABLING THE INTERNET OF THINGS, A WORLD IN WHICH CONSUMERS AND BUSINESS ENJOY RICH NEW SERVICES CONNECTED BY INTELLIGENT AND SECURE MOBILE NETWORKS.

The security of connected devices in a large scale network depends on all stakeholders following a unified approach.

The GSMA published IoT Security Guidelines, a set of best practices for the secure end-to-end design, development and deployment of IoT solutions on any mobile network. Based on the expertise and collective knowledge of the mobile telecommunications industry, the guidelines offer valuable insights and recommendations to enable the creation of trusted, reliable and scalable IoT services.

The GSMA IoT Security Assessment scheme enables IoT companies to demonstrate that their products are aligned with the GSMA guidelines. The scheme covers security controls for the whole ecosystem and further enhances the alignment of all stakeholders by putting in place a concise framework with consistent terminology and a structured approach to IoT security information. By submitting an assessment, IoT companies can demonstrate the security measures they have taken to protect their products and services from cyber security risk, enhancing their reputation as trusted IoT service providers.

To find out more visit: www.gsma.com/IoTSecurity