News

N° 77

gmv
INNOVATING SOLUTIONS

Cybersecurity coming up trumps

INTERVIEW
Guillermo Llorente Ballesteros
MAPFRE's Corporate Security Manager

ISO 27701 Sustainable Privacy Management

The economy is now going through an unprecedented digital transformation. A key aspect of this process is mass data mining for defining data-driven customer-centric business models and strategies.

Protection of personal data comes into its own here, not only as a binding obligation under the GDPR, CCPA and Spain's data protection law, etc, but also because any violation of privacy could hit the business's reputation hard.

Guaranteeing privacy, however, enforcing privacy regulations, is no cakewalk. Factors like speed of change, complexity of the environment, the business-process scale, etc, all force the costs skywards; they also make for a piecemeal approach.

There is now a pressing need for a sustainable privacy-management model.

marketing.TIC@gmv.com

gmv
INNOVATING SOLUTIONS

Letter from the president

The other day I opened an email attachment. I scan read the message and clicked on the attachment. It could have been a virus, ransomware or any other type of malware. Luckily it was a harmless awareness-raising message.

For over a quarter of a century now GMV has been developing services and solutions for ascertaining the cybersecurity level, managing the technological infrastructure and governing its clients' cybersecurity processes. The need to set up defenses against cybernetic attacks is common to all types of diverse interconnected systems, calling for a specific solution to suit each particular case. GMV boasts a wealth of experience and has come up with solutions to protect not only major corporate networks but also ATMs, medical services, industrial systems and satellite control centers.

This year's pandemic has clearly brought out the potential of digitalization not only to boost productivity and use resources more efficiently but also for companies to keep up business despite the lockdown by way of teleworking. The downside of teleworking, however, is increased vulnerability of companies and public organizations to cyberattacks, the number of which has soared during the pandemic. We all run a higher risk privately too, since we have had to switch many of our social activities to online alternatives. All users across the board therefore need to keep their guard up to pinpoint and avoid the new risks in this scenario. Because cybersecurity is a technological race against cybercrime, in which the human being is all too often the weak point.

Mónica Martínez

N° 77

Published
GMV

Editorship-Coordination
Marta Jimeno, Marta del Pozo

Area Heads
Antonio Hernández, Miguel Ángel Molina, José Prieto, Javier Zubieta

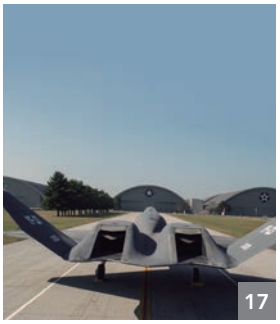
Writing
Alberto Águeda, Luis Javier Álvarez, António Araújo, Carlos Barredo, Mariano J. Benito, Filipe Brandão, Antonio Cabañas, Francisco Cabral, María Jesús Calvo, Jesús Cegarra, Maole Cerezo, Ana Cezón, Cristian Corneliu, Luis Manuel Cuesta, Marco Donadio, Iulia Dragomir, Raquel Fernández, Teresa Ferreira, Javier Fidalgo, Alberto de la Fuente, Hugo Garzón, Javier Gómez, Mariella Graziano, Sara Gutiérrez, Juan Ramón Gutiérrez, Sergi Güell, Ana Herrera, Filipe Henriques, Héctor Herrero, Javier Hidalgo, Aurora Izquierdo, Rafał Krzysiak, Cristina Liébana, Fátima López, Jesús Alejandro López, Arturo Martín, David Merino, Carlos Molina, Daniel Montero, Cristina Muñoz, Héctor Naranjo, Jorge Ocón, Eric Polvorosa, Isidro Prieto, José Prieto, Beatriz Revilla, Pablo Rivas, Eugenio Sillero, Antonio Tabasco, Tatiana Teresa, Maria Victoria Toledano, Manuel Toledo, João Vitorino

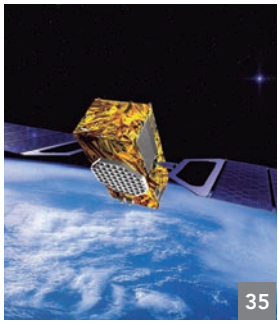
Art, design and layout
Paloma Casero, Verónica Arribas

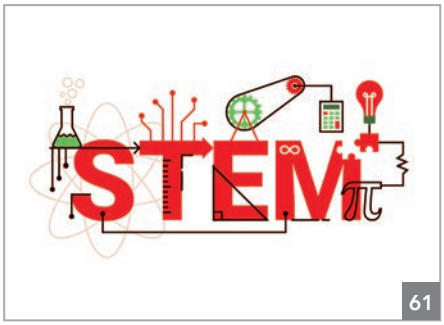
MORE INFORMATION
marketing@gmv.com
+34 91 807 21 00

Magazine N°. 77. First quarter of 2021

CONTENTS







Cybersecurity coming up trumps

The coronavirus pandemic has thrown us pell-mell into a new worldwide scenario in which our ways of socializing, prioritizing, looking at things in general and of course working have all been revolutionized. When all this is over we are likely to get back to a situation similar to the one we knew before. It is equally likely that the systems we have turned to perforce, such as teleworking, which has proved its mettle in these troublesome times, become part of our daily routine.

Cybersecurity, in each of its facets, has proved its worth at all levels. Everything seems to suggest that we have now "crossed the Rubicon" with no going back, and the digitalization process will only pick up speed from here on. This is being driven by various factors, which we look at below.

One of the standout factors on a personnel level is the abrupt irruption of a new way of working from anywhere rather than the normal worksite. The word "teleworking" existed before but it has now come into its own and taken up a whole new meaning. When the lockdown hit, it did not wrong-foot everyone the same. GMV has found that those companies that were previously running a tried-and-tested business continuity plan were better prepared for the new situation. In the months of January and February 2020, for example, when the writing was already on the wall, some firms were able to set up a continuity plan. This enabled them to run a teleworking stress test, stockpile material or redouble the number of technological contingency tests. This readiness softened the impact and boosted the lockdown resilience.

Furthermore, some of GMV's clients were in the same pre-lockdown situation, so we were all able to get mutual feedback on the practices we were all rolling out. Both GMV and several of its clients, for example, decided to switch some of their activities to teleworking even before the lockdown was declared, even before the family-disrupting school closures.

It is therefore well worthwhile to set up standard-defined management systems in general, and in the particular case in hand, a business continuity plan. Cybersecurity coming up trumps.

SECURE TELEWORKING

Under this new situation GMV has been well aware that the so-called "corporate perimeter" has been scattered to the winds; if anything, it is now delineated by the private router of each worker. This raised qualms at first. As weeks went by, however, the cyber-threat proved to lie elsewhere.

From a technological point of view organizations have been able to implement many cyber-protection measures to safeguard the teleworking infrastructure. True it is too that many organizations have found serious loopholes and lingering vulnerabilities. It is now a good time for those organizations that downplayed and underestimated the importance of cybersecurity during the teleworking rollout to check and improve these systems. Any outlay in vulnerability management always pays off in the end.

Teleworking with built-in cybersecurity is therefore compatible, complementary and necessary. Cybersecurity coming up trumps.

EVER-LATENT CYBER-THREATS

Cyber-threats are proving to be particularly virulent in two scenarios of this pandemic. Firstly, at corporate level, which has been hit by waves of ransomware attacks. Even though we could almost call it "business as usual" for these cybercriminals, their impact has been higher than on other occasions. In this economically shaky 2021 we need to bear firmly in mind that some disinvestments can turn out to be expensive even in the short term, with cybercriminals always on the prowl. The last thing we need now is to have to struggle with service outages or information theft.

Secondly, the private sphere. Cybersecurity comes across as difficult and technological to the layman, bristling with threats and fears. This is very offputting to the private individual, who tends to shy away from cybersecurity until a cyber-incident occurs. Small wonder, therefore, the proliferation right now of massive phishing campaigns by email, SMS or Whatsapp with click bait of all types. On the plus side, our growing digital exposure means we tend to be better informed; cybersecurity knowledge is easier to come by. Witness the huge number of training sessions given online and free in these months, plus the top-quality educational material made available also without charge to one and all. This awareness-raising effort is unprecedented: Cybersecurity coming up trumps.

HEALTHCARE CYBERSECURITY

Many people have turned to the internet to find out more about the pandemic and its successive waves. Society was mad keen to know more about a potentially lethal virus. At the same time the health system came under great stress, running out of room for the sick and exhausting the health workers themselves; they even came to refer to the situation they were living through as a "war".

Even before the pandemic hit, healthcare care data was already one of the hottest items on the black market, vying for first place with banking and personal data. The pandemic only made it more cherished. Organizations in charge of generating and keeping this data came into the crosshairs of the cybercriminals. Major healthcare corporations have indeed suffered attention-grabbing incidents.

Over a year has passed since we were goggling at the speeded-up images of a prefabricated mega-hospital being built in China. On the threshold, hopefully, of herd immunity, thanks to the Herculean effort of scientists and the pharmaceutical industry, "pandemic fatigue" has now become the buzzword.

The initial anxiety sparked off by the onset of the virus has now been joined

by an impatience to be vaccinated and the fatigue brought on by months of wearing facemasks, angst about the harrowing rate of cases and deaths, house arrest, municipal closures, news programs in which SARS-CoV-2 hogged all the headlines. All this has whipped up a sense of vulnerability that cybercriminals continue to exploit ruthlessly.

WITHOUT WASTING TIME

On 23 March 2020, right in the middle of the lockdown, the national police reported an attempt to block the computers of Spanish hospitals by sending health workers emails with a "very dangerous virus" designed to break into medical centers' IT systems.

The concern generated by a potential outage of our hospitals' information systems is reflected by the parliamentary question that the Ministry of the Interior had to answer last October: "so far in 2020 the National Cybersecurity and Infrastructure-Protection Center (Centro Nacional de Protección de Infraestructuras y ciberseguridad: CNPIC) has unearthed three serious healthcare cyber-incidents, one of them targeting a critical operator". It should be pointed out here that, according to the findings of a recent report by Check Point Research, Spain's infection rate is the third highest in the whole world, behind only Canada and Germany.

Another milestone event at world level was the Red Cross letter signed by leading figures from commerce and politics like the Presidents of Telefónica and Microsoft and the former presidents of Brazil and Colombia. The letter was the brainchild of the CyberPeace Institute (a non-government brokered by Microsoft, the Hewlett Foundation, MasterCard and other major corporations and philanthropic institutions, which aims to protect cybernetic attack victims and help them to recover afterwards). The letter urged governments to recognize that "cybernetic operations against health centers are unlawful and unacceptable", also calling on civil society and the private sector to join forces to ensure that medical facilities are respected and protected. "We don't tolerate attacks on health infrastructure in the physical world and we must not tolerate such attacks in cyberspace" runs the text. On a world level, it should be pointed out, attacks against health firms have risen by 45% since the onset of the pandemic.

OUR COMMITMENT

GMV in keeping with its status as a leading managed security services firm with its inhouse computer emergency response team GMV-CERT, is well aware of the threats. Its Cyberthreat Intelligence Team has now joined its forces with the fight against cybercrime in the country's health sector, keeping a permanent track on any malicious activity. As a result of this constant monitoring activity, and on the basis of the observed behavior in the first two waves of COVID cases in Spain, GMV published the report "Ciberamenazas susceptibles de afectar al sistema sanitario español" (Cyberthreats likely to affect Spain's health system), warning health service providers, pharmaceutical companies, insurers and health centers of the cyberattack risk. The latest ransomware attacks have shown cybercriminals' prime target to be the data kept in patients' medical records, information on new drug-development, clinical trials, industrial property, etc.

This report announced back in April that "Between 60 and 70% of threats use social engineering as their entry vector, taking advantage of human weakness and curiosity, need of information and fear of COVID-19 or an altruistic urge to help or find out more". GMV also laid down in the report a series of recommendations to keep health service providers, pharmaceutical companies, insurers and health centers on their toes.

FROM OUR VANTAGE POINT

With care home residents, healthcare workers, law enforcement officers and other priority groups inoculated, we are now facing up to a new wave unleashed by new strains of a virus that have already caused over 2.6 million deaths around the world. Doubts and anxiety remain, moreover, about when the rest of the population will be vaccinated; it is a time of political turmoil too. According to GMV's experts this is a perfect hotbed for organized cybercrime groups.

The monitoring carried out by GMV's Cyberthreat Intelligence Team bear out this claim. In 2021 so far the team has unearthed campaigns to access elderly persons' homes, infiltration of malware into healthcare institutions or other institutions that are playing a vital role in the current context and supply-chain sabotage attempts.

In 2020 an increase was observed in the number of attacks on the health sector and government authorities. Furthermore, COVID-19's digital knock-on effect has been worldwide, and in Spain especially there has been a sharp increase in online frauds and swindles in comparison with the previous year.

Spanish government bodies like national insurance, the taxation authority or road traffic authority, among others, have fallen prey to phishing campaigns that aim to perpetrate fraud or spread malware. Others have suffered serious incidents, even having to close down due to ransomware lockups. The security panorama at world level should be a concern not only to cybersecurity experts and firms like GMV. There is now an increasingly well-armed cybercriminal industry ready to exploit any weakness found in the systems of major firms or government organizations; witness the hacks of SolarWinds, VMWARE or Microsoft Exchange servers. All this suggests the situation will only worsen in the rest of 2021.

Juan Ramón Gutiérrez, Head of the Forensic and Threat Intelligence section of GMV's Secure e-Solutions sector

CONTINUOUS MONITORING

It is nowadays becoming increasingly easy to pick up "ransomware as a service" versions on the black market. In today's fraught scenario this is becoming a matter of increasing concern, especially as these attacks are also tending to become more aggressive. Campaigns of phishing and smishing preying on SMSs or any other e-texting method are the quickest, most efficient and even cheapest method of spread. They tap into social engineering strategies to gull users with messages designed to pique their curiosity, fear or other sentiment related to SARS-CoV-2 and the vaccination campaign.

Our Cyberthreat Intelligence Team's constant monitoring of cyberspace and monitoring of internet gives us a special insight into the state of play. From this vantage point we would argue that vaccination is now the major worldwide concern. It seems to be becoming clear that it is also the weak point exploited by cybercriminals, without downplaying other pandemic-related issues such as lockdown-compensation payments. Alongside, cyberfraud in the form of mock parcel-delivery messages on SMS, email, whatsapp continue apace too. Internet purchases have soared during the past year; this upward trend looks set to continue and is proving a fertile field for cybercriminals.

One of the weakest flanks of the vaccination campaign is the supply chain (Laboratories Logistics Vaccination Centers / Hospitals) where threats are also piling up. Social engineering arguments are used to perpetrate attacks against any of the supply-chain stakeholders. Phishing attacks on one of these stakeholders favor infection of the information systems of the rest. These are now being increasingly seen too. Remember that we are talking about priceless data that is critical for human life. They therefore easily lend themselves to blackmail in the form of ransom demands or sale on the black market.

In 2021 other stakeholders, though not completely new on the scene, came into the cybercriminals' crosshairs for the first time. The appearance of different vaccines around the world, under the aegis of the various blocs (USA, Europe, Russia and China), ushers in a whole host of political, economic and even supranational interests. Vaccines now represent an unseemly tussle for geostrategic advantage and no bloc wants to be left behind in the race.

REINFORCING OUR DEFENSE SYSTEMS

Early detection is one of the most efficient protection methods, bringing the threat-intelligence data into relation with known vulnerabilities in any organization's perimeter or internal assets. Ongoing user awareness-raising is vital too. After all, once the malware or ransomware has managed to infect any of the organization's internal computers, conventional monitoring systems can only identify and contain infected machines due to the rapidity of infection between network computers (lateral movements).

It has to be borne in mind here that today's ransomware has an "explosive phase" or the moment when a host of infected computers suddenly show up after a period of silent propagation flying under the radar. This is what makes it so dangerous and stresses the importance of threat intelligence as a preventive means, giving us a technical edge over the cybercriminals.

Just as with the COVID-19 pandemic or any other biological virus the infections of computer systems (digital) have their "patient 0" or index case, after which their propagation capacity (lateral movements) is unlimited unless contention measures are taken. Hence the prominence of phishing campaigns as the main vector in the infection of digital systems and the prime importance of not opening any message or notification of an alarmist character that might arrive by email, whatsapp message or any other type of e-messaging system including the short message service (SMS).

If in doubt please take time to check elsewhere the veracity of any message before opening any attachment of clicking on any link within the message. Remember that no government authority or bank would ask us to interact with them by means of a messaging service. There is no doubt that COVID-19 vectors and the vaccine imbroglio represent a perfect storm for organized crime; stories are now rife about cybersecurity incidents and the growing sophistication of the deception methods. Identify theft of services seen as trustworthy by users, whether individuals or organizations, in order to lull them in to the trap, will be the tonic during 2021.

We know all too many examples of attacks that bring an organization grinding to a halt, often translating into a headline-grabbing nationwide news item. As in the famous tale of Little Red Riding Hood, we experts have been calling wolf for some time now but it is not until cybersecurity upsets like this occur that people will realize we are not spinning a yarn here.

Guillermo Llorente Ballesteros

MAPFRE's Corporate Security Manager

He is Infantry Lieutenant Colonel, holder of the Chief of Staff Diploma and Joint Chief of Staff Diploma on leave of absence.

After holding various unit-command posts, especially in international missions, he came to the security world during his commander post, holding for six years the post of Head of the Counterintelligence, Interior Security and Army Personnel Unit, with the award of diverse decorations.

He joined MAPFRE in 2006, currently holding the post of MAPFRE's Corporate Security Manager overseeing all physical and logical security areas, plus business continuity, crisis management and data privacy.

Group MAPFRE's integral security model has been hailed as an example of success by the technological consultancy firm Gartner and has won several prizes and distinctions on the strength of its innovating character. These include the first prize of the Guardia Civil "Duque de Ahumada a la Excelencia en Seguridad Corporativa".

He is a habitual speaker at conferences and colloquia and is also professor of several security-related Master and Post-grad courses at different universities.

You have been one of the great advocates of the need to seek synergies between physical and logical security. What is your take on the convergence between them?
The essence of our security model is its client centeredness, aiming to provide them with a uniform and consistent protection against threats of any type, regardless of their size.

This model offers a large number of benefits. First and foremost it favors the securing of synergies between the attack-vector combatting measures and the security dimension. Secondly, it favors uniformity of the protection model, avoiding inequality or inconsistency of the measures taken in the various ambits.

This global approach also favors two key security processes: planning and crisis response monitoring. With this outlook I see it as possible to define more efficiently the moment and mode in which attack-prevention measures should be applied and how strongly. An overarching vision has allowed us to coordinate the crisis response, moving the levers of each vector uniformly, coordinately and in keeping with this purpose. It makes no sense at all to come up with an independent response to each vector when the attack is being launched simultaneously against many of them.

In conclusion, and in my opinion, only by way of integrating physical and logical security and the information obtained from them will we be able to provide efficient and effective protection against the new threats.

This approach poses a technological challenge: working with different sources of information from the physical and logical world. How ready are corporations for this?
From our vantage point we see that we corporations in general still have a long way to go and are uncertain as yet about the best way of integrating the information from the different systems. This means not only integration of elements from the logical and physical world, although some solutions are forthcoming here in terms of innovations like video camera logs, common access cards, etc, but also the formidable challenges within the digital world itself, such as efficient management and centralization of information obtained from the different clouds of the various vendors. Migration to the cloud has added on a further degree of complexity to an already highly complex situation.

MAPFRE is a worldwide-trading company. What security challenges does this geographical dispersion pose and how are you tackling it?
MAPFRE is trading in almost fifty countries. This is a priceless factor, enriching the whole group, but it does pose a stiff security challenge for the management teams, especially the sheer size of the operation.

The main difficulty thrown up by our global profile is providing a uniform security to all our colleagues and our whole network, regardless of where the assets and information systems

are. We can never afford to take our eyes of the ball here for one minute.

And in pursuing this goal we have to be allow for local idiosyncrasies like human teams' adaptation speed, their size and cultural differences or the business activities each company carries out. This calls for a certain flexibility and fleet-footedness. All makes an already huge challenge even more forbidding.

Last but not least, together with the need of establishing a uniform standard and remaining flexible enough to adapt as necessary to the different scenarios, we come up against a factor that complicates our activity even more: the patchy and often prolix legislation of each different country MAPFRE trades in.

What role does security play within MAPFRE's organization? What services do the rest of MAPFRE demand from the security department?
Our outlook is that security is part and parcel of any organization and should imbue it throughout. It is not just a question of coming to the plate during crises; we security departments have to be part of the organization's lifeblood rather than an ad hoc tag-on.

In MAPFRE's model, of which we are very proud, security forms part of the life of any organization in all its dimensions. This means that we in security feel ourselves to be an essential link in the organization, and it favors our alignment with the company's overall strategy. It also empowers us to endow all the company's activities with efficient security. Design-up security, after all, is simpler and cheaper to implement than tagging it on afterwards.

In MAPFRE's model security imbues the whole organization

What level of active demand for services do you see from the rest of the company?
Internal demand has grown nonstop, especially over the last five years due to two crucial factors. Firstly, the company as a whole has taken the importance of security to heart after all the awareness-raising plans and programs we have carried out. Secondly, society as a whole is more aware of its importance too. Milestone developments like the General Data Protection Regulation (GDPR) have raised people's awareness of data protection and privacy to a whole new level.

These two factors, higher internal awareness and the higher general awareness driven by the media and other stakeholders (auditors, interest groups, etc.), have naturally tended to increase the security demand in any project.

For our part we have been able to respond to our colleagues' demands. We have been receptive to the needs, acting as enablers of their work, always with the overriding aim of providing law-abiding, ecofriendly security. This demand has been growing permanently, as a result of all the above; this makes us satisfied about how well we are integrated into the company's life.

Which cybersecurity initiatives would you stress as the most important?
The biggest challenge we face now is to boost our cloud response and monitoring capability. The company's technological watchword is "cloud first". Under this premise the digital transformation process and the migration to the Cloud has perforce to coexist with an "on premise" facet that can never completely disappear; it has its own organic growth process and still underpins critical processes of the company.

In this coexistence model we have to strengthen our response to cloud hosted assets and the ability to monitor them, doing so quickly and in a decisive, no-nonsense way. Cloud hosting is bound to follow an upward trend and it calls for a security level in keeping with current risks. The challenge lies in finding the way of bringing this in efficiently.

At this moment cybersecurity is a vanguard knowledge area. The book about how to get things done in each scenario hasn't been written yet. The current situation requires us to provide security in a context of high volatility and enormous technological complexity.

The pandemic has been another turn of the screw in this complexity you mention. How has this stage affected MAPFRE from the cybersecurity point of view? What have these last few months meant for you personally?
We'll all agree that this pandemic is a global drama, both human and economic, and we can never forget the millions of people who have died from COVID. Without ever losing sight of this human tragedy, for those of us who are working in security teams it has been a professional challenge. We are permanently on a crisis management footing. Crisis management is a big part of MAPFRE's remit; we are ready and trained for this ... We are working each year on business continuity and contingency plans to be ready for these situations whenever they crop up.

From this viewpoint this crisis has given us security professionals the chance to show our worth to the firm, showing what all those hours of training, economic resources and dedicated personnel have been in aid of. MAPFRE has been capable of keeping the service going at all times and in every country it trades in. We have also been capable of achieving the goals we set ourselves from the very first minute of this crisis. The primordial goal was to protect our employees in the best way possible, and our collaborators, suppliers and clients too. Secondly, ensuring that business goes on for our clients and, thirdly, supporting society.

These three goals have been achieved with a high degree of fulfilment and satisfaction. This gives security professionals a legitimate and intimate sense of job well done, of having come up to scratch in the face of such a sterling challenge.

You have indeed overcome the challenge with flying colors, and this is due largely to the preparatory work you mention. A crisis of this type also offers a chance to learn. Which would you cite as the main cybersecurity lessons we have learned from this experience?

Several security lessons have been learned. The first thing we did was roll up our sleeves and get down to work, to deal with the immediate contingency, after which the crisis dragged on for much longer than we would have imagined beforehand.

This has reminded us of one of the basic crisis-management principles; black swans do exist and real scenarios are worse than you might imagine in the planning.

The east-to-west spread of the pandemic, from China through the Philippines, Italy, Spain, America... gave us sufficient time to assimilate the lessons learned from the crisis response in the areas where it first appeared, obtaining synergies. MAPFRE's global vision and situation kick-started our anticipation capacity, looking at the territories where we have offices, activating the crisis management strategy in each geographical area even weeks before the governments recognized this situation.

More lessons learned: firstly, the need of separating off device access from the user's physical location; secondly, the philosophy of zero trust and the security safety-net concept have both come to stay. We have set up the double-authentication factor – linked solely to certain users, to certain critical pre-pandemic environments – for MAPFRE users around the world. The essential need of setting up a uniform security model as mentioned above, or the need of knitting it into all business areas before and during the crisis to be able to give them the service they are asking for.

Which vulnerabilities and threats would you highlight on the risk map as it's been evolving over recent years?

We've been talking about the increasing threat level for years: the growth in ransomware and service-denial attacks; the rash of phishing campaigns... These threats have been increasing both in amount and sophistication.

Firms of all size are now taking up and using technology intensively. This makes us all increasingly dependent on our systems and data, and hence vulnerable to hackers.

In previous stages banks were the main target; now, insofar as the hackers are capable of denying services, stealing data or denting the reputation and extorting us all, we have all been brought into the hackers' sights. This increase in the trawl of possible targets has enabled cybercriminals to scale up their business and encouraged many more to try their luck.

There is yet another attack-boosting factor, namely the reduction in the risk run by hackers. These attacks can now be made from remote, unknown sites, using tools that hitherto did not exist, like botnets, which enable computers to be used for fraud, unbeknown to their users. The appearance of cryptocurrencies has thrown thicker veils over capital flows coming from criminal activities like extortion, physical theft, data theft. This helps hackers to monetize their operations more quickly and more safely.

Lastly, companies' digital transformation process itself is generating a greater dependence on and use of digital assets. The number of connected devices grows nonstop; add the pandemic to the mix, with its concomitant increase in teleworking, and the result is a vast increase in companies' exposure surface. In short, a perfect storm. The rate of threats has now picked up an unprecedented speed.

Would you say that the cybersecurity regulations enforced in the countries where you operate are enough to protect organizations like yours?

Regulation is necessary to allow states and governments to create a secure environment where citizens' data is protected from a risk that has only increased in recent times.

I would advocate a more uniform, less patchy regulatory framework laying down clear rules and striking the right balance without slipping into overregulation. Level playing fields for all would also favor free competition, a sine qua non of progress in our society.

> Cybercriminals now have a much wider trawl of targets, enabling them to scale up their business and encouraging many more to try their luck

In all countries MAPFRE trades in there is a huge amount of regulation, much of it working from very similar principles but with nuances and idiosyncrasies that call for significant powers of adaptation.

The working relationship between MAPFRE and GMV has been forged over many years. What aspects of this joint work would you highlight?

The relation between MAPFRE and GMV dates back fifteen years, with growing collaboration ever since.

We at MAPFRE look for long-term relations underpinned by trustworthiness. Security environments, after all, are volatile with growing needs of crisis response. GMV has shown over these years to be a trustworthy company boasting a vast knowledge of the cybersecurity market and cutting-edge technology.

We have found in GMV the support and responsiveness we've needed at moments of crisis, showing great adaptability in meeting our needs and helping us to forge the path we have chosen to follow, a path we need to define together with inspiring and insightful partners. GMV has also given us something we value enormously, its wealth of expertise and experience.

We certainly have no hesitation in expressing our heartfelt gratitude for the support we've received from GMV over these years.

GMV achieves full incorporation into the early phase of NGWS/FCAS

This contractual amendment enabling Spanish industry to join fully in Phase 1A Technology Demonstrators activities of the NGWS/FCAS project paves the way for signing of the corresponding contract with Airbus D&S GmbH, leader of the Remote Carriers Technology Pillar

Last December, thanks to the excellent spadework of the Spanish MoD, France's General Armament Directorate (*Direction Générale de l'Armament*: DGA), acting on behalf of the governments of Spain, Germany and France, formalized the contractual amendment permitting Spanish industry's full integration into Phase 1A Technology Demonstrators activities of the NGWS/FCAS project, which was initially launched by France and Germany in early 2020.

This contractual amendment facilitated the signing of the corresponding agreement with Airbus D&S GmbH (leader of the Remote Carriers Pillar), also in December, which ushered GMV, through the joint venture UTE SATNUS, into Phase 1A of this technology pillar. This pillar focuses on the development of new technologies and assessment of new concepts, doing so in coordination with NGWS/FCAS's new manned combat aircraft, based on a set of unmanned vehicles.

The contract corresponding to this phase covers the activities to be carried out during the first 18 months, geared towards the development of diverse demonstrators and technology maturing tasks, with the maiden flights being penciled in for 2026.

GMV will be inputting its expertise built up from a long track record in international industrial cooperation projects. This rests on four main pillars: direct contracting with European agencies and NATO; the sale of JISR products; direct participation in R&D programs, and GMV's cooperative spirit, always keen to collaborate not only with the rest of industry but also the main technological research centers.

GMV's participation centers on the technologies it has been working on incessantly over recent years, building up a cast-iron reputation in sectors such as navigation, avionics, autonomous systems and artificial intelligence.

The FCAS program, one of Europe's biggest defense projects, aims to develop a "system of systems" connecting interoperable manned and unmanned air platforms.

At the same time, also within the SATNUS consortium, GMV is busy drawing up the bid for the follow-on phases 1B and 2.

New version of the ADS-B monitoring system for ENAIRE

GMV has handed over to Spain's air navigation authority, ENAIRE, a new version of the APRESTA system for monitoring the performance of the ADS-B surveillance system in Spain, under the framework contract awarded by ENAIRE to GMV back in 2019 for developing and maintaining APRESTA.

APRESTA facilitates real-time collection and processing in ASTERIX format (All Purpose Structured Eurocontrol Surveillance Information Exchange) of the data generated by several ADS-B stations. It also allows for periodic generation of performance reports to check whether the ADS-B surveillance service provided in a given airspace meets applicable ADS-B standards (ED-129B).

Another standout APRESTA feature, based on GMV's ***GNASSURE*** product, is detection and tracking of areas where GNSS performance has been degraded by radio frequency interference (RFI), whether deliberately or otherwise, from any system or device located on the overflown terrain.

Any GNSS degradation events are also periodically reported by APRESTA while an alert service notifies registered users of any deviation from predicted ADS-B performance or any detected GNSS problem. Last but not least APRESTA includes a web interface allowing for simultaneous access by several users for the purposes, among other possibilities, of enquiring about the system state, downloading the abovementioned periodic reports or generating ad hoc reports.

APRESTA has been developed in close collaboration with ENAIRE, whose expert knowledge of how the ADS-B system works has enabled GMV to develop bespoke algorithms to suit this particular purpose.

GNSS performance forecasts for navigation applications and aeronautical surveillance

In 2020 EUROCONTROL awarded GMV a three-year contract for forecasting GPS/RAIM outages and generation of Notices to Airmen (NOTAMs) for aerodromes operating with GNSS-based instrument flight procedures. Six months of this contract have now run their course.

This service, going under the name of AUGUR, is made available free by EUROCONTROL to pilots, airspace users (e.g. airlines), and air navigation service providers (ANSPs). It consists of two main elements.

Firstly, the website (*https://augur.eurocontrol.int/help/*), which allows any user to find out about forecast GPS/RAIM outages for the next three days in any airport located in ECAC and MEDA member states. Secondly, an interface for automatically sending NOTAM proposals associated with these outages. These NOTAM proposals are sent to the European AIS database (EAD) for subsequent publication in each country's NOTAM Office (NOF) for consultation by aeronautical users in each case.

The ECAC and MEDA regions pool 44 European countries and 12 countries of North Africa and the Middle East, respectively. In all they take in over one thousand airports scattered around the whole world, including the overseas colonies of several European countries.

GMV's service includes hosting the system that provides the abovementioned services, its maintenance and also an AUGUR user help-desk.

This service is based on GMV's inhouse ***GNASSURE*** product, which provides GNSS performance forecasts for use in aviation navigation and surveillance applications (e.g. ADS-B).

Spanish elite units receive the first SEEKER RPAS units

By the end of 2020 the Spanish Army and Navy received the first SEEKER Remotely Piloted Aircraft Systems (RPAS). SEEKER is the unmanned aircraft that will boost the intelligence-, surveillance- and reconnaissance-capabilities of the Spanish Army's 6th "Almogávares" Paratroopers Brigade (*Brigada "Almogávares" VI de Paracaidistas del Ejército de Tierra*) and the Marine Infantry Protection Force (*Brigada de Infantería de Marina del Tercio de Armada*), two elite forces that enjoy international renown and prestige.

SEEKER, one of the most efficient of any RPASs, boasts a 90-minute endurance, a 15-km range, and weighs in at 3.5 kg. In Spain the aircraft and its systems have been designed by GMV and Aurea Avionics; it was totally manufactured on Spanish territory, and this proved crucial when it came to mitigating the effects of the broken supply chains at the start and middle of the year.

Despite the COVID-19 epidemic the manufacture, test flights and delivery of the aircraft were all performed within the project deadlines, thanks to a switch in working methods and a reorganization of the activities by the personnel of both firms and the MoD.

SEEKER will provide BRIPAC (Paratrooper Brigade) and BRIMAR (Marine Infantry Brigade) with real-time thermal-infrared and visible-spectrum video, augmented by metadata that can be mined in situ by the operators and remotely by the command and control centers. This is due to the new ground-station architecture, which has been completely digitalized to make SEEKER compatible with NATO's standard command centers. Any allied force will therefore be able to integrate the aircraft directly into its fleet and command centers, adding on versatility and ensuring joint operability between all troops and systems. This gives a wholly Spanish product a strong international projection, allowing it not only to form part of the ongoing modernization project of Spain's armed forces but also to play its full part in the growing cooperation and collaboration of Europe's defense industries.

The RPAS has been financed by the Subdirectorate General of Planning, Technology and Innovation (*Subdirección General de Planificación, Tecnología e Innovación*) of the Directorate General of Armaments and Material (DGAM) as part of the Spanish MoD's RAPAZ program.

GMV improves the RPAS autonomy range

The definition phase has recently given way to a new phase of SAFETERM, a European Defense Agency project being carried out by GMV in collaboration with AERTEC.

SAFETERM system is aimed at enhancing current Medium Altitude Long Endurance (MALE) and large tactical Remotely Piloted Aircraft System (RPAS) Flight Termination Systems and procedures. The SAFETERM system will provide the RPAS with a higher level of autonomy for emergency situations, particularly those involving the loss/degradation of the command and control link along with other failures. More precisely, SAFETERM enables a safe termination of a flight in case of failures, both in terms of autonomy and remote pilot control capability, through the determination of Alternative Flight Termination Areas to avoid human or assets damages.

In this phase, the project team will improve the SAFETERM demonstrator using real avionic hardware and software. A certifiable processor platform will be selected for the design and the software will be divided into partitions on a certifiable RTOS. Whereas no real certification activities for the development are envisaged, the certification procedures will be used as a guidance for Machine Learning training and verification metric extraction. The main assurance focus will be placed on the development and acceptance of the classification algorithm.

For the flight data gathering, a flight campaign is planned, using AERTEC's TARSIS-75 aircraft. The aim of these flights will be recording videos of different terrain characteristics at different altitudes and at different lighting conditions (flights will be performed during the morning, noon and afternoon to get different sun conditions). Each recorded video will be split into two image sets to be used for training and validation independently.

Another relevant aspect of the project is related to the certification and standardization support activities. GMV is currently a member of the SAE G34 / EUROCAE WG 114, Artificial Intelligence in Aviation Joint International Committee, which looks towards the compliance for the certification of Artificial Intelligence (AI) within safety critical aeronautical systems.

Future Civil and Military Operations using Unmanned Aerial Vehicles

On 4 February GMV held the webinar "Future Civil and Military Operations using Unmanned Aerial Vehicles", presented by Carlos Molina, Project Head of GMV's Avionics Division.

This seminar dealt with recent progress in the use of unmanned aerial vehicles in both the civil and military spheres. Some of the most important concepts in the former are U-Space and Urban Air Mobility (UAM). Carlos Molina ran through various civil applications in which unmanned aerial systems are being used today as well as future use cases of these systems, such as aerial taxis.

Various inhouse GMV U-Space service developments included in the ***dronelocus***® suite were also presented, as integrated in the demonstrator of the ENAIRE-coordinated U-Space project DOMUS.

This presentation also threw the spotlight on the most important breakthroughs in unmanned aerial system use in the military sphere, where vehicles of this type are bound to play a crucial role in future defense programs. Various military applications were mentioned and explained together with the most important technological challenges posed by the future development of unmanned aerial systems in the defense arena.

Finally, Carlos Molina talked about some of GMV's standout UAS contributions in various defense programs, such as the supply of several SEEKER unmanned aerial systems to the Spanish MoD as well as GMV's participation in the SATNUS consortium, national coordinator of the FCAS remote carriers pillar.

GMV studies the integration of AI into aeronautic GNC systems

The European Defense Agency (EDA) awards GMV the AI-GNCAir project, the remit of which is to study the new Guidance, Navigation and Control (GNC) technology for air-platform systems

In the aeronautics sector, and in particular in guidance, navigation and (GNC) systems, sensor data has to be processed in such a way as to ensure a high level of integrity, detecting and preventing the propagation of incorrect readings or external interference in order to improve the precision, integrity and availability of solutions.

AI comes into its own here, recognizing signal interference and incorrect sensor readings or forecasting missing data as a result of this interference and incorrect readings. The race is now underway, therefore, to improve GNC systems, not only to boost performance but also to achieve a dynamic sensor reconfiguration by determining data quality and detecting underperforming sensors.

In this context the European Defense Agency (EDA) has awarded GMV the AI-GNCAir project, the remit of which is to study the new Guidance, Navigation and Control (GNC) technology for air-platform systems. This endeavor is part of the implementation of EDA's strategic research agenda within CapTech GNC, looking at how Artificial Intelligence technology might be integrated into GNC systems and the roadmaps needed for closing the associated technological gaps in the EU.

AI-GNCAir, led by GMV and carried out in collaboration with the Madrid Polytechnic University's Research Center into Information Processing and Telecommunications (*Centro de Investigación en Procesado de la Información y Telecomunicaciones de la Universidad Politécnica de Madrid*: UPM-IPTC), will focus on intelligent data fusion for AI-driven absolute and relative localization in avionics GNC systems.

AI-GNCAir will look into the state of the art in the use of intelligent data fusion for self-localization of air-vehicles. The purpose is to recommend a generic GNC architecture for safely using AI supported algorithms in the aeronautical domain. On a second iteration of the project, a use case will be simulated for comparing the performance of the new algorithms as opposed to the traditional data fusion techniques.

GMV consolidates its Space Traffic Management leadership

GMV chosen by the European Commission to lead a coordination and support action (CSA) for presenting future European-capability-development proposals in space traffic management (STM)

GMV, European leader in Space Situational Awareness (SSA) and Space Surveillance and Tracking (SST), has been chosen by the European Commission to lead a Coordination and Support Action (CSA) within the H2020 program to make proposals for a future European Space Traffic Management (STM) capability: EUSTM.

Space activity has increased exponentially in recent decades. The emergence of new public and private actors, plus new concepts such as small satellites and large constellations, orbiting satellite services, reusable rockets, etc, all pose new challenges. The number of objects in orbit is likely to increase drastically, and it is therefore necessary to develop capabilities to manage them in an efficient manner. An increasing need for a policy and legal framework supported by the

required technology developments has also emerged to foster and ensure the desired security, safety, sustainability and stability of space operations. These frameworks are broadly known as Space Traffic Management (STM) while the technology supporting is referred to as Space Situational Awareness (SSA) or Space Surveillance and Tracking (SST).

Europe greatly benefits from the open policy of the U.S. federal government in terms of accessing SSA/SST data and services by means of dedicated SSA Data Sharing agreements. To ensure sovereignty, autonomy and leadership in this domain whilst reducing this dependability, the European Commission started to work on an independent SSA/SST capability.

EUSTM´s objective is to strengthen the European public and private space sector, encourage an innovative, competitive, and profitable space industry, as well as a research community that develops and runs space infrastructure. EUSTM will roll out an innovative collaborative platform to encourage the exchange of information among team members and also relevant external stakeholders. This platform's goal is to create an active community of interest that will be an endless source of STM information for the EC.

The GMV-led EUSTM consortium is made up of the following18 European industries and institutions: Weber-Steinhaus and Smith (Germany); Europaisches Institut fur Weltraumpolitik (Austria); Spacetec Partners SRL and Qinetiq Space NV (Belgium), GomSpace (Denmark); Satellite Center of the European Union, ENAIRE, Payload Aerospace, SL (Spain); Iceye Oy (Finland); Eutelsat SA, PriceWaterhouseCoopers Advisory SAS, Office National d'Estudes et de Recherches Aerospatiales, Safran and Université Paris-Saclay (France); AVIO SPA (Italy); and Universitaet Bern, Clearspace SA, Sceye SA (Switzerland).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004319

This article reflects the author's view and not necessarily the views of the European Commission or of the EU Research Executive Agency

GMV to supply the ground segment of EUTELSAT's new satellite fleet

EUTELSAT has once more turned to GMV for implementation of its control center known as NEO, a bespoke version for EUTELSAT of GMV's inhouse ***Hifly***® product, plus the FOCUS flight dynamics system, based on the ***Focussuite*** product portfolio for its next three missions: Konnect VHTS, Hotbird 13F and Hotbird 13G.

Konnect VHTS is a satellite belonging to Spacebus Neo family built by Thales Alenia Space as part of a new generation of Very High Throughput Satellites (VHTS). Hotbird 13F and 13G, for their part, are two new satellites of the Eurostar Neo platform built by Airbus Defence and Space to replace the former satellites of the Hotbird orbit.

EUTELSAT, one of GMV's flagship clients, runs GMV-developed systems for controlling its complete fleet of satellites, featuring the aforementioned multiplatform satellite control systems and NEO multi-satellite and the FOCUS orbital dynamics systems, plus state-of-the-art payload management systems.

The long-lasting and solid relation between GMV and Eutelsat, dating way back to the first contract award in 1993, has been forged by a large number of hardworking people who have spared no effort to achieve top-quality results. This team has been renewed over time but has managed not only to keep up this unflagging, never-say-die spirit but also boost the business carried out for Eutelsat.

GMV's systems supplied under this contract will see to ground operations management of these three new satellites, which are scheduled to be up and running and ready for ground System Validation Tests (SVTs) in the first months of 2021.

Türksat 5A satellite launch

After passing successfully the System Validation Tests (SVT), Türksat 5A satellite was successfully launched on 8 January 2021 at 02:15:00 UTC from Cape Canaveral (CCSFS)´s SLC-40.

GMV provided support to Airbus DS (manufacturer) and Türksat (prime) during the SVT and the launch for the deployed software for SCC (Satellite Control Center): ***Hifly***©, Flight dynamics system and ***Smart rings***.

Türksat 5A satellite is based on the latest electric orbit raising (EOR) of Airbus' highly reliable & cost-efficient Eurostar E3000 platform, which uses electric propulsion for in-orbit raising and station-keeping. EOR will take up to 4 months before the final orbit raising.

Türksat 5A is a broadcast satellite which will operate in Ku-band transponders at the 31 East longitude slot in geostationary orbit, covering Turkey, the Middle East, Europe, North Africa and South Africa. The spacecraft has a launch mass of 3,500 kg and electrical power of 12 kW, the expected on-orbit life time will be 15 years.

Validation of Galileo's authentication service

Galileo initiates the Open Service Navigation Message Authentication (OSNMA) signal-vetting phase. OSNMA, together with the high-precision service, is one of the Galileo constellation's main added values

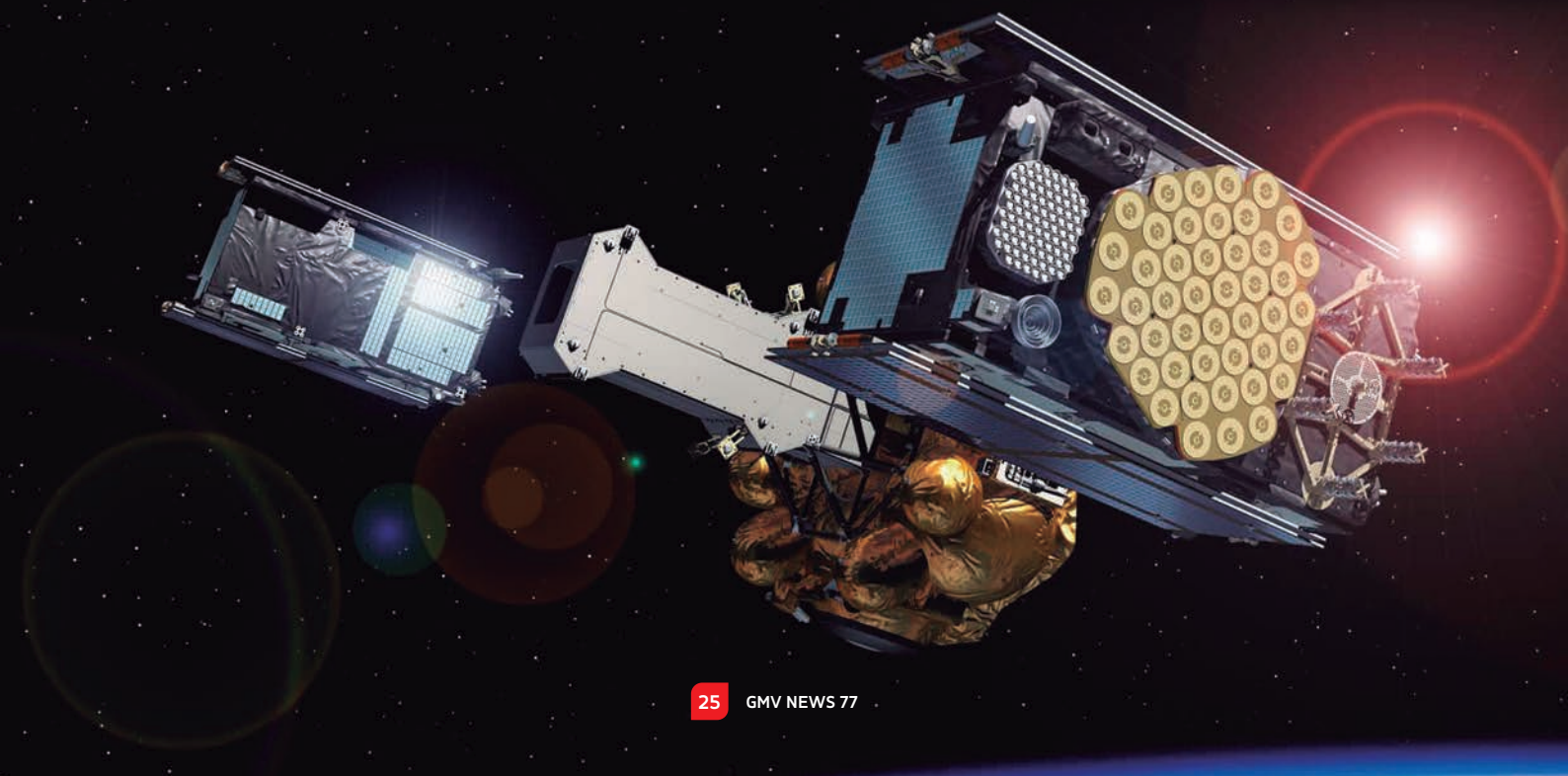
An important milestone came recently for Europe's GNSS and also for the worldwide GNSS community. In November Galileo started the testing phase of the Open Service Navigation Message Authentication (OSNMA) in the signal-in-space. The European GNSS Service Centre (GSC) is currently responsible for generating the OSNMA message and delivering it to the Galileo's Ground Mission Segment. The OSNMA is, together with the High Accuracy Service, one of the main added values provided by the Galileo constellation.

The GSC forms part of the infrastructure of Europe's Galileo navigation program. Its main role is to act as the single interface with EGNSS users and contribute to OSNMA and High Accuracy service delivery. The centre is also conceived as a centre of expertise to facilitate the exchange of knowledge, to support developers, to bring GNSS to wider notice and to provide support for the provision of value-added services.

The GSC, located in Madrid, is run by the European GNSS Agency (GSA) with the support of Spain, which provides the Galileo program with the necessary infrastructure and facilities for hosting the centre. In 2014 a GMV-led consortium together with Indra won the framework contract for supply of GSC infrastructure, holding onto this responsibility ever since. Since that year, GMV also led the AALECS (Authentic and Accurate Location Experimentation with the Commercial Service) project, for the European Commission that implemented the first OSNMA prototypes.

The new version of the GSC, supporting the OSNMA testing phase, is now operational. OSNMA ensures that the received navigation data is coming from a Galileo satellite and is not being faked. This verification layer provides a strong feature of protection for the Galileo constellation. This is a great achievement for Europe's GNSS; it is the first signal from a constellation of navigation satellites that demonstrates this service worldwide, making Galileo the most robust and secure GNSS system. This new GSC version allows the Galileo Programme to prepare the future OSNMA Public Observation phase.

The GSC Infrastructure consortium has played a major role in this great success, highlighting GMV's work and reaffirming its position as a dependable partner. During the implementation phase, the consortium has been working closely with the GSA and other stakeholders, such as the European Commission, to develop the GSC, upgrade Galileo's services and win Europe's GNSS worldwide leadership in the field of secure and robust navigation.



GMV probes the synergies between fundamental physics and PNT systems

Positrino, a European Space Agency (ESA) project carried out by a GMV-led consortium, has recently been completed. Its remit was to study the feasibility of a neutrino-based Positioning, Navigation and Timing (PNT) system.

Neutrinos are fundamental particles of standard particle physics, interacting very weakly with matter and traveling practically at the speed of light. They can therefore reach places that are beyond the reach of GNSS signals, such as underground or underwater environments. A neutrino-based PNT system could therefore come in very handy for such purposes as submarine or spacecraft navigation or mining applications.

The one-year project also proposed a high-level design of a system based on artificial sources of isotropic neutrinos and miniaturized neutrino detectors. Several simulations of particle physics and PNT performance have been carried out to weigh up their feasibility.

Positrino has shown that, in view of the current neutrino-generation and -detection technology and the breakthroughs being achieved in this particle technology, a neutrino PNT system could be feasible in the short-medium term.

In the upcoming months ESA is scheduled to contract new technical activities to consolidate high-level design of a system of this type, as well as carrying out proofs of concept to pave the way for operational development once the technical and economic feasibility has been proven.

GMV is playing a key role in ESA projects (led by the Galileo Science Office in ESAC, Madrid) to harness synergies between fundamental physics and PNT technology. GMV is also priming the consortium of the Lifeline project, initiated in November 2020, for a study of the feasibility and high-level design of a relativist positioning system, in other words, a PNT system naturally incorporating Einstein's theory of relativity.

Renewal of the framework contract for the Copernicus border surveillance service

The objectives of this service are to reduce the number of undetected illegal immigrants entering the EU, reduce the number of deaths at sea and boost the European Union's internal security as a whole, helping to head off cross-border crime

GMV is part of the consortium that recently won the framework contract issued by the European Union Satellite Centre, for continuing with the provision of the Copernicus border monitoring service. GMV has been working on this service since the beginning of operations in 2015.

The goals of the service are to reduce the number of illegal immigrants entering the EU undetected, to reduce the death toll of human lives at sea and to increase internal security of the European Union as a whole by contributing to the prevention of cross-border crime. The service supports the EU's external border surveillance information exchange framework (EUROSUR/FRONTEX) by providing near real time data on what is happening on land around the EU's borders.

The developed products consist of reference maps which include a wide range of observable features extracted from Earth Observation and open source data, and provide a background of geographical context and representation of countries' areas, including hydrography, topography, land cover, infrastructure and population activities. According to user need/requests, VHR images (acquisition date and time, cloud cover, resolution, among other criteria) are acquired as needed and used to extract updated information. The maps are generated at very-large-to-large scales (1:5,000 - 1:100,000).

The products are provided as vector and cartographic outputs (layouts), represented within a single map sheet in portrait or landscape format and at different page sizes (A0 to A2).

GMV presents its Woodland plague-damage detection system

On 21 and 22 January GMV took part in the seminar "Bark-beetle damage in the SCERIN domain: detection, monitoring and associated Land Cover Change dynamics" organized by the South-Central European Regional International Network (SCERIN) for the Global Observations of Forest Cover and Land Use Dynamics (GOFC-GOLD).

This seminar focused on the impact of bark-beetle outbreaks in the forests of Central-Eastern Europe. This beetle attacks the trees' bark, debilitating them to the point of death. When its population reaches plague level it could devastate vast swathes of woodland, producing huge environmental and economic losses.

Ángel Fernández, Earth Observation Data Scientist of GMV's Remote Sensing & Geospatial Analytics division, talked about the use of Sentinel-2 satellite data for detecting bark-beetle damage in Europe's forests highlighting the development and results of GMV's biotic damage product. This technological solution, developed under the GMV-led European project MySustainableForest, looks for, detects, delimits and estimates woodland plague damage using machine-learning techniques.

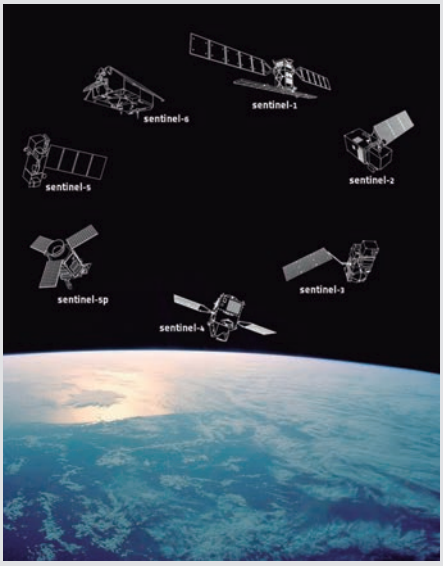
A study on the impact of these plagues was also presented in a paper called "Monitoring Bark Beetle Forest Damage in Central Europe. A Remote Sensing Approach Validated with Field Data", published in October in the journal Remote Sensing and drawn up by GMV with the collaboration of Mendel University in Brno (Czech Republic), another member of the MySustainableForest consortium.

GMV a habitual participant in conferences as key stakeholder in the Space Downstream sector

As a key player in the space downstream sector, GMV has been called to participate in several webinars and events held in Portugal.

In November 2020, within the "Encontro com a Ciência e Tecnologia" promoted by the national institutional actors through the Minister of Science, Technology and higher education, Teresa Ferreira, GMV's director of Space in Portugal participated in a round table to discuss the European Commission's proposed Space Program. Teresa stressed GMV's strong role in the downstream while giving a national industrial perspective of the program and its strategic importance and impact on the national economy.

Early in 2021 GMV was again called to showcase its capabilities in the Copernicus program and in particular in the use of earth observation information for the provision of applications and services to our society. Within the marine workshop, Filipe Brandão presented the study case entitled "Pollution – detection and monitoring of marine litter" while in the land workshop, António Araújo, GMV's Project Manager in Portugal showcased GMV's capabilities in Emergency Management – Risk Mapping and Recovery.



GMV looks into the installation of the new Copernicus observatory in the Arctic

The dramatic decline of the ice cover in the Arctic Ocean opens up new economic opportunities; new traffic routes can now be navigated, goods transported and unexplored natural resources accessed. On the downside there are serious concerns about the environmental threats and security challenges deriving from the intensive exploitation of natural resources in the Arctic sea and the surrounding coasts.

The risk of seaborne disasters like oil spills or the proliferation of new seashore infrastructures might undermine European security. The EU consensus to maintain a multilateral cooperation approach to ensure stability and dialogued solutions in the region triggers an increasing demand for situational awareness within the EU.

In this context a new Horizon 2020 project has just begun: the Arctic Observatory for Copernicus Support to External Actions Service, ARCOS. The objective of ARCOS is to design and implement an early-warning system capable of providing continuous monitoring over the Arctic Region and operative products for the security domain; the system aims at integrating space and non-space data sources as well as thematic products from existing Copernicus services.

GMV is participating in the project on-board the e-GEOS led consortium, together with the EU Satellite Centre, the Meteorological Institute of Finland, the Polytechnic University of Milan, the Finnish ICEYE SAR constellation operator and the Danish consulting COWI.

ARCOS products will service three scales of information needs: firstly, automatic early warnings triggering alarms under certain conditions; secondly, user-driven alerts, based on indicators required by the users; thirdly, geospatial intelligence products of the previous products which require expert analysis.

The project faces data-processing challenges, ranging from the wide area to be monitored to the extreme light conditions and satellite observation angles. The project plans to test artificial intelligence disruptive techniques for automatic feature extraction and analytics.

ARCOS security applications include domains such as marine resources exploitation (aquaculture, illegal fishing), secure transports and communication (connectivity, autonomous shipping, logistics) and maritime spatial planning (coastal protection, renewable energy, port infrastructures).

Model-Checking for Formal Verification of Space Systems

Model-based systems engineering (MBSE) is the adopted practice for taming the increased complexity and heterogeneity of today's (systems-of-) systems under development. Integrated in a model-driven development process, such as the waterfall model, and supported by many tools, MBSE provides a complete solution that aims to derive, possibly (semi-)automatically, implementations from high-level specifications.

TASTE (*https://taste.tools/*), developed by the European Space Agency, is a pragmatic MBSE tool which puts together a number of technologies that cover a large spectrum from data and behavioral modelling to automatic generation of binary application for embedded systems.

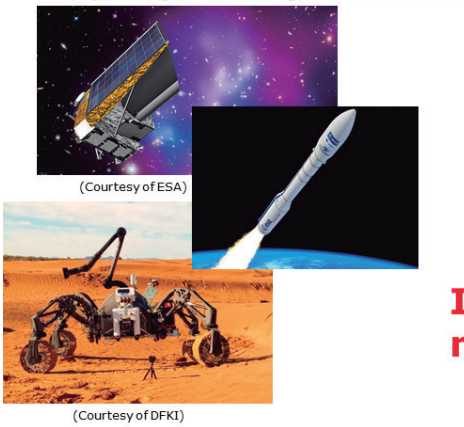
GMV has recently started working on the MoC4Space project. The aim of the project is to integrate within the TASTE tool a model-checking approach that will automate the verification of complex functional properties for embedded space software systems.

Model-checking is a formal verification technique which exhaustively checks whether the desired system property is satisfied or not. The solution to be implemented in the project relies on the IF toolset (*https://www-verimag.imag.fr/~async/IF/index.html*) as model-checking backend. Then TASTE/SDL designs and the modelled properties are translated to the IF language and the model-checking is applied. The results obtained are represented on the TASTE model, especially when counter-examples (behavior invalidating the property) are generated.

Several challenges will be addressed during the project, such as: the modelling of system properties (stop conditions, Message Sequence Charts and observers) in TASTE, the definition of the formal execution semantics of TASTE, the transformation between TASTE and IF models, and the seamless integration of the approach within the TASTE GUI. Finally, the implemented approach will be validated on two space representative case studies: a flight-embedded system and an autonomous space robotics exploration system.

The MoC4Space project is being led by GMV with subcontractors, Universite Toulouse II Jean Jaures and CNRS/ VERIMAG.

Space systems designed with **TASTE**



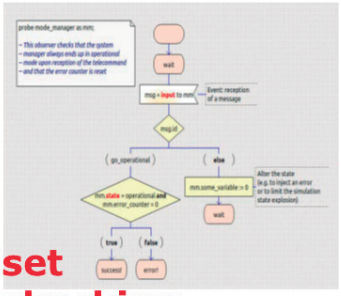
(Courtesy of ESA)

(Courtesy of DFKI)

⊨ ✓

IF Toolset model-checking

Functional system property (as SDL statemachine)



Digital transformation applied to precision agriculture and remote sensing

Agriculture is nowadays living through a digital transformation, bringing in more productive, efficient and sustainable forms of farming.

First came the steam-driven mechanization of much farming work; next came electricity and fossil fuels. The third revolution, dubbed the green revolution, was ushered in by improved seeds, fertilizers and phytosanitary products, soon joined by a spectacular development of heavy machinery for all sorts of farming tasks. And now comes the fourth revolution with the phasing in of new ICTs, especially Big Data and Artificial Intelligence (AI).

Under the overarching title "Towards the fourth agrarian revolution", Cajamar hosted in January several seminars looking into the detail of this new revolution. GMV took part in one of these to talk about its expertise in agrofood digital transformation, specifically in remote sensing and precision agriculture.

Miguel Hormigo, Industry Manager of GMV's Secure e-Solutions sector, and Antonio Tabasco, head of remote-sensing and geospatial analysis, talked about the smart-farming solutions GMV has been working on recently, such as AI to classify images or trace assets, before zooming in on the concrete example of ***Wineo***, an advanced geospatial data analysis service to support decision-making in agriculture.

GMV develops a remote marine litter detection methodology

GMV has developed a groundbreaking approach based on remote data for detection of marine litter, using satellite images and machine-learning techniques

Marine-litter, resulting from spills and bad waste management, has now become a worldwide problem. More than half this waste is plastic, and this is bad news for the oceans as it takes so long to break down, up to 1000 years. In terms of both amount and composition it therefore represents a serious global threat to marine and coastal ecosystems.

GMV has developed a groundbreaking novel synthetic data-based approach to this problem, based on remote sensing of marine waste using Sentinel-2 satellite images from Europe's Copernicus Earth-Observation (EO) program and machine-learning techniques. This EO data analysis and processing method detects possible marine debris, being able to classify and quantify according to pixel-level litter fraction present. The first tests of detection and identification methods of plastics like PET have already been carried out. Several projects are now in development and validation phase, most notably BEWATS, ATIN-BLUECO and PLESS.

GMV, in collaboration with Vigo University and Spain's Mathematical Sciences Institute *(Instituto de Ciencias Matemáticas*: CSIC-UAM-UCM-UC3M), is carrying out the BEWATS project. The aim is the detection, monitoring and traceability of marine waste (macroplastics and others) washed up on the beaches and other coastal areas of Galicia (Spain). The overarching idea is to seek solutions to this problem and establish more efficient clean-up strategies using new information sources. BEWATS is being funded by the Programa Pleamar of the Biodiversity Foundation (*Fundación Biodiversidad*) of Spain's Ministry for the Ecological Transition and Demographic Challenge (*Ministerio para la Transición Ecológica y el Reto Demográfico*).

The Blue Economy project (ATIN-BLUECO), led by GMV and funded by the European Space Agency (ESA), sets out to develop and demonstrate EO-driven data solutions that deliver actionable information on marine-litter and oil spills, among other applications, to key coastal stakeholders. This project is focusing on the geographical area of Vigo Port in Galicia (Spain), Açores (Portugal) and in Argentina.

Last but not least, in February 2021, GMV began priming the ESA-funded Plastic-Less Society (PLESS) project in collaboration with the Research Centre of IST for Marine, Environment and Technology (*Instituto Superior Técnico, Lisboa*). PLESS looks into the technical and economic feasibility of using space applications to help reduce the environmental impact of plastic litter.

As well as these projects, GMV has also validated this approach in other sites of Europe, South America and Africa, tapping into open data on marine-litter.

GMV gives a progress report on CYBELE pilot tests

GMV is participating in CYBELE, an EU-funded project that aims to generate innovation and create value in the domain of agri-food by applying Precision Agriculture (PA) and Precision Livestock Farming (PLF) methods.

Right from the project kickoff GMV has been leading one of the nine demonstrators to weigh up and show the usefulness of PA and PLF technology, concentrating on the development of climate services for organic fruit production.

Due to the sheer complexity of forecasting extreme-weather events, the trials, held in late January, were broken down into three blocks: hail forecasting, frost forecasting and the phenology of each type of fruit.

Working on this demonstrator, GMV has achieved notable headway in the conceptualization and exploration of machine-learning methods for forecasting frost and hail. These demonstrator trials were carried out in two zones of Valencia region.

GMV's work on this demonstrator draws on data from the Meteorological Archival and Retrieval System of the European Centre for Medium-Range Weather Forecasts (ECMWF) and the Spanish Meteorological Agency (*Agencia Española de Meteorología*: AEMET).

GMV present at the European Space Conference

In mid-January the European Space Conference was held online, a yearly event that brings together top representatives from industry, the government, European and worldwide agencies and institutions to take stock of the space sector.

GMV sponsored this 13th conference, held under the banner theme of "Space Embracing a Changing World: Green, Digital, Resilience & Security". The event debated such issues as the space industry, New Space, space exploration missions, aviation and maritime-transport applications, telecommunications and 5G, the digital-transition challenge, quantum technology breakthroughs, AI and the European recovery strategy.

GMV's SEO, Jesús B. Serrano, took part in the presentation "The role of research in boosting European space competitiveness", together with EC Director General for Research and Innovation, Jean-Eric Paquet; ESA's Director of Technology, Engineering and Quality and head of ESTEC, Franco Ongaro; ESRE President, Bruno Sainjon, and Telespazio CEO, Luigi Pasquali. Another GMV executive, Space General Manager, Jorge Potti, formed part of the parallel session "Cleaning up our orbits: accelerating the move to remove space debris", sharing the panel with ESA's Director of Operations, Rolf Densing; the Chief of Committee, Policy and Legal Affairs Section of the United Nations Office for Outer Space Affairs (UNOOSA), Niklas Hedman, and D-Orbit CEO, Luca Rossettini.

Other important public figures included the President of the European Council, Charles Michel; diverse Commissioners and High Representatives of the European Union, Spain's Minister of Science and Innovation, Pedro Duque; ESA's Director General, Jan Wörner, and his successor, Josef Aschbacher.

GMV consolidates its leadership in the third phase of the EC's biggest space robotics program

GMV's performance in the first and second phase of the Strategic Research Cluster (SRC) in space robotics technology has now won it the role of strategic partner in the three new projects resulting from the third call

The European Commission (EC) has recently announced the three new third-phase projects of the Strategic Research Cluster (SRC) on space robotics technologies, coordinated by the PERASPERA project under the Horizon 2020 program (H2020).

The first phase of this ambitious, groundbreaking endeavor involved six projects (three led by GMV) to tackle the design, manufacture and testing in representative environments of various high-performance robotic Common Building Blocks suitable for operation in orbital or planetary space projects. The main objectives of the second call, now drawing to a close, are the integration of the previously prepared Common Building Blocks for space robotics resulting from the first phase into demonstrators on ground, targeting specific applications of space robotics in the field of orbital and planetary (Lunar-Martian terrains) use.

The remit of this third call, as far as on-orbit servicing missions are concerned, is, to take one more step towards a final demo in an orbital mission. Secondly, as far as planetary-exploration missions go, it aims to develop a robot-collaboration demonstrator in a Mars-like terrain.

GMV's performance in the first two phases has won the company the ranking of strategic partner in these three new projects: CoRoB-X (Cooperative Robots for Extreme Environments), EROSS+ (European Robotic Orbital Support Services +) y PERIOD (PERASPERA In-Orbit Demonstration), taking on responsibility for critical systems like the robotics components' autonomy systems and cooperation capability, while also contributing towards the guidance, navigation and control (GNC) systems.

CoRob-X, led by DFKI, will develop and demonstrate enabling technologies for multi-agent robotic teams, with the ultimate aim of improving inter-robot collaboration. The two projects European Robotic Orbital Support Services + (EROSS+) and PERASPERA In-Orbit Demonstration (PERIOD), led by Thales Alenia Space and Airbus Defence and Space GmbH respectively, will design two mission concepts of in-service demonstration and in-orbit assembly with the aim of providing a European system to cater not only for satellites providing this service but also the service-receiving satellites. All this will be based on the robotics technology developed in H2020 calls 1 and 2 of the space robotics SRC.

GMV's crucial role in these three projects confirms its European leadership in OBA (On-Board Autonomy) and GNC (Guidance, Navigation and Control) for orbital and surface applications.

The ADE rover ready for use in nuclear scenarios

■ On 12 March the ADE rover was put through its paces in a nuclear scenario.

ADE (Autonomous DEcision Making in very long traverses) is a European-Commission-funded robotics project included in the second phase of the Strategic Research Cluster (SRC) in Space Robotics Technologies. Its remit is to develop and test a rover system with very long traverse capabilities (building up to a 1-km run in less than 6 hours) by independently taking the decisions required to progress, reduce risks and seize opportunities of data collection. Although the project's main focus is a planetary exploration rover it also includes an additional use case geared towards the terrestrial robotics market; this involves an autonomous robotic system to be used in nuclear-plant decommissioning tasks.

The platform used in the test was GMV's inhouse Foxizirc rover, fitted with an additional ADE-running processor known as ADAM. ADAM is a module that increase's the rover's autonomy, allowing for automatic 3D mapping in the form of a Digital Elevation Map (DEM), without the need for any previous map. This mapping algorithm, updated in real time, is robust against scene changes, allowing the rover to avoid any new obstacles that might crop up in its path. The system is capable of automatically detecting "hot points" of higher radiation, completely analyzing the area under study and drawing up a final map showing the radiation levels at each point. It is also capable of analyzing ground-level leaks by means of convolutional neural nets trained up to automatically detect water leaks or any strange elements in the area to be explored.

The event was followed online by a team of project reviewers belonging to the PERASPERA (H2020) group, made up by various representatives of Europe's space agencies (ESA and the UK Space Agency) plus members of the European Commission. Onsite were representatives of Spain's Industrial Technological Development (*Center Centro para el Desarrollo Tecnológico Industrial*: CDTI).

GMV is a new member of the Spanish Association of Robotics and Automation

■ GMV joins the Spanish Association of Robotics and Automation (*Asociación Española de Robótica y Automatización*: AER Automation), further cementing its position as one of the main players in the automation and industrial-robotics market.

The remit of AER Automation associates is to promote the transformation of the national manufacturing fabric on the strength of automation and industrial-robotics technology.

In the words of Miguel Hormigo, Industry Manager of GMV's Secure e-Solutions sector, "we are delighted and proud to become members of such a prestigious organization as AER Automation. Forming part of a grouping with major companies and experts helps us all to get behind the digital transformation of the industrial sector".

GMV participates in the kick-off of the European GEODE project

GEODE (GalilEO for EU DEfence) project is a crucial and decisive step towards the development of the Galileo Public Regulated Service (PRS) military User Segment. It is also one of the most ambitious defense cooperation projects ever launched under the umbrella of the European Commission's EDIDP program

As part of the consortium, led by FDC, the technology multinational GMV has participated in the GEODE Kick-Off meeting held on February 8.

GEODE (GalilEO for EU DEfence) is a crucial and decisive step towards the development of the Galileo Public Regulated Service (PRS) military User Segment and one of the most ambitious Defense cooperation projects launched under the umbrella of the European Commission's European Defence Industrial Development Programme (EDIDP). Co financed by Belgium, Germany, Italy, France and Spain, GEODE is supported by the EU with a grant of about 44 million Euros.

GEODE aims to boost the EU industry's competitiveness in the highly strategic domain of military positioning, navigation, timing and synchronization (PNT) and to endow EU military forces with Galileo Public Regulated Service (PRS) capacity. The project will be implemented by a Consortium of 30 undertakings from 14 EU countries.

The Spanish industrial team, made up by GMV, Indra and Tecnobit, takes on first level responsibility for the complete development of the solution for naval military platforms (GNSS/PRS receiver with security module and CRPA antenna). GMV is responsible for the integration of the GNSS/PRS Receiver system and, in particular, for the development of all the receiver's signal-processing, navigation and timing functions.

GEODE will provide the EU Industry with an even playing field in the Defense PNT market, where military GPS's essentialness at the moment ensures US Industry's supremacy. It will also reinforce EU military capability and autonomy and maximize the benefits of the Galileo program by promoting take-up of its crucial PRS service.

This project has received funding from the European Defence Industrial Development Programme (EDIDP) under grant agreement No EDIDP-PNTSCC-2019-039-GEODE

This article reflects only the author's view. The Commission and the EU Member States involved in the Geode project are not responsible for any use that may be made of the information it contains

GMV phases new features into the Spanish Navy's SMACS program

In late 2020, in the Spanish navy's Maritime Surveillance Operations Center (*Centro de Operaciones de Vigilancia Marítima*: COVAM) in Cartagena, GMV successfully deployed SMACS adaptor phase 3 (Spanish Maritime Affairs Cross Sectorial IT Interoperability Improvement).

This new phase, awarded by the Navy Logistic Support Office (*Jefatura de Apoyo Logístico de la Armada*), showed its ongoing commitment to supporting the Common Information Sharing Environment (CISE) for exchanging maritime safety and surveillance information in Europe.

The project's first phase kicked off as an adaptor to permit information exchange at national level between the navy's COVAM systems, the Fishery Monitoring Center (*Centro de Seguimiento Pesquero*: CSP) and the Operational Coordination Center (*Centro de Coordinación Operativa*: CECOP); since then it has been upgraded without fail year after year.

The first of the feats under this project was to turn the Spanish Navy into a CISE nexus with the maritime surveillance network MARSUR, involving the participation of military organizations from 20 countries.

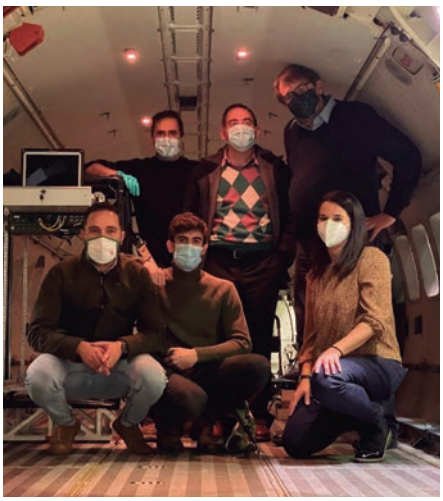
The next breakthrough came in the form of connection with MAJIIC JISR standards, areas in which GMV boasts a wealth of experience thanks to the family of Coalition Shared Database (CSD) products developed for the Spanish MoD.

In this last phase an adaptor behavior analysis module has been added on, flagging up ships making suspicious maneuvers. Maneuvers of this type, such as ships entering or leaving a given zone or the near approach of two ships at sea, will trip an alarm to indicate the irregular activity to the operator.

Among the navy's priorities feature the encouragement of tools that favor collaboration and improve available information. GMV and the navy therefore continue to work together to improve the system and turn it into a key aid for operators' daily tasks, all in the interests of ensuring maritime safety.

A new milestone in intelligence, surveillance and reconnaissance

At the end of 2020 the reception was held for development of a CORE-type mountable computer interface for cooperative Electronic Support Measure (ESM) operations.



Project team after completing the hardware integration tests

The objective of this project is to supply a system for exploiting Link16 track information plus information from the new electronic warfare pod of the Spanish airforce's F-18, dubbed CORE (short in Spanish for "Electronic Recognition Operational Capability"). The system will be able to operate both from land and onboard a new aerial platform for a Signals Intelligence (SIGINT) mission, such as a C-295.

The reception comes after a complex campaign of tests held in ALA-35 (Getafe Airbase) and in the Experimentation and Armament Logistic Center (*Centro Logístico de Armamento y Experimentación*: CLAEX) of Torrejón Airbase. These tests checked system interoperability in a scenario designed to represent the destination (F-18 communication components, JISR network and communication protocols of the POD-CORE ground station).

GMV's system will pick up ESM tracks from different sources, then performing fusion processes and generating messages for Cooperative ESM Operations (CESMO) under the interoperability standard STANAG 4658. Thanks to the use of this standard the MoD's systems can be integrated into multinational missions with sensors and processing nodes of allied countries.

The Spanish Seaports Authority turns once again to GMV

GMV renews the maintenance contract for the AIS-receiving stations of the Spanish Seaports Authority (*Puertos del Estado*), phasing in new features to improve port running and the management of navigation aids

For yet another year the Spanish Seaports Authority (*Puertos del Estado*) has entrusted maintenance of its Automatic Identification System (AIS) stations to GMV.

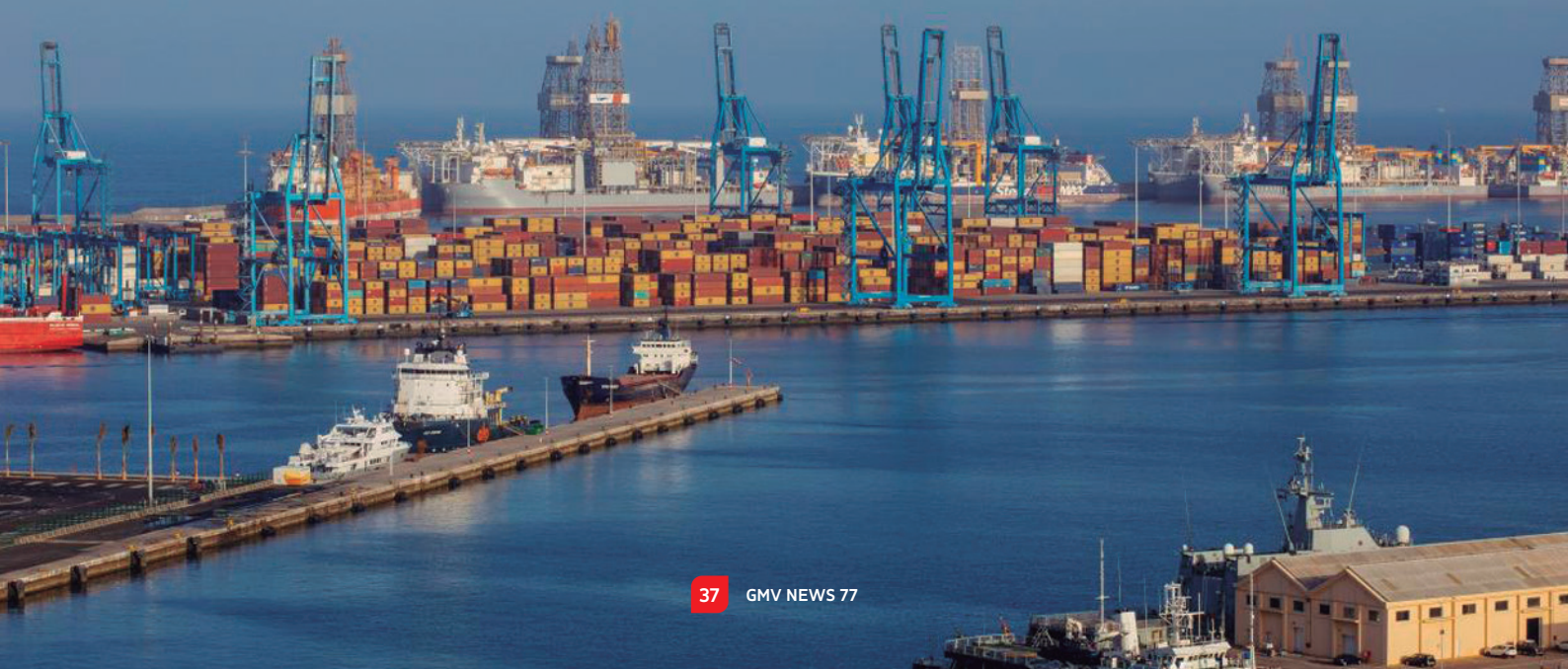
The remit of Puertos del Estado's AIS network is to give data users valuable real-time ship information such as position, bearing, speed, type of cargo, destination port and arrival time plus other analog information, helping them to run ports and manage navigation aids. Furthermore, all the information that arrives is stored so it can be used afterwards for the purposes of statistical analysis, investigation of incidents or conducting port-operation and planning studies.

All the information recorded daily by the Puertos del Estado network on over 3000 ships in Spanish waters is displayed in GMV's inhouse ***ShipLocus***® application. This information, issued by the ships' onboard AIS devices is received by several coastal stations, also maintained by GMV.

As well as helping *Puertos del Estado* to run its operations and navigation aids, this information can also be shared with other organizations like the Guardia Civil, the Spanish Navy and *Salvamento Marítimo* (Maritime Rescue Service).

Besides the port- and maritime-traffic monitoring and observation functions, the network also provides ships with a varied range of services, such as exchanging messages with ships for use by port control centers, the broadcasting of weather and oceanographic information from *Puertos del Estado's* reading network, sending warning messages to ships for them to avoid collisions with beaconing or wave-measurement buoys, and the sending of messages to ships to warn them of any navigation aid incidents.

Under this new contract ***ShipLocus***® will report the real-time and recorded messages given by the different types of ships in the various navigation stages.



GMV one of the go-to firms for EUCI networks and systems

In late 2019 the European Defense Agency (EDA) awarded GMV a multiyear framework contract for design and rollout of communication and information systems (CIS) for storing, processing and interchanging classified information (EUCI) up to EU SECRET level.

EDA's aim is to set up EUCI-CISs capable of handling classified information both at internal level, within EDA, and sharing it with government organizations and institutions of EU member states and other stakeholders involved in projects requiring this information.

Under this contract GMV, as system integrator, will be the single point of contact; it will also be the company responsible for establishing and analyzing system- and user-requirements, assessing threats, vulnerabilities and risks, identifying the corresponding mitigation measures, drawing up the necessary documentation for the accreditation process and supporting its performance. It will also be responsible for the design, implementation and deployment of said systems.

Durante 2020 GMV worked on the design and certification-preparation of the first of the systems. To be deployed, accredited and cleared for operation during 2021, this system will allow the agency to handle classified information up to EU SECRET level.

At the same time, in early 2021, a second system for handling information up to EU RESTRICTED level entered its preparation- and design-phase and is scheduled to be brought into operation in early 2022.

The systems are being designed and deployed in due accordance with the EU legal framework for handling and exchanging EUCI, with final clearance by the Security Accreditation Authority (SAA) of the General Secretariat of the Council (GSC).

After rollout GMV will then take on responsibility for providing maintenance and technical-support services and training up EDA personnel who will be running the systems.

GMV participates in the EDA intelligence, surveillance and reconnaissance workshop

In June 2019 the European Defense Agency (EDA) published eleven Strategic Context Cases (SCCs) as a guide for implementation of the European Capability Development Priorities as agreed by member states back in 2018.

These SCCs are being used to define investment priorities of future European defense initiatives, such as Permanent Structured Cooperation (PESCO) projects and the European Defence Funds (EDF).

In this context EDA is organizing a series of workshops for each SCC in order to inform industry of the corresponding SCC and glean contributions for additional definition of the working lines in the area concerned.

On 21 January the first online workshop looked at information superiority, in particular intelligence, surveillance and reconnaissance capabilities. The paper "Intelligence, Surveillance and Reconnaissance Networked Capabilities", prepared by GMV, was one of the six selected to be read in the workshop before representatives of governmental organizations, industry and academia; it was heard and received with great interest.

Activities of this type enable GMV's defense industry business to go from strength to strength; so strong, in fact, that the company has by now become an influencer in deciding the priority investment lines of Europe's new defense programs.

Opinion

The NIS Regulation approved in Spain

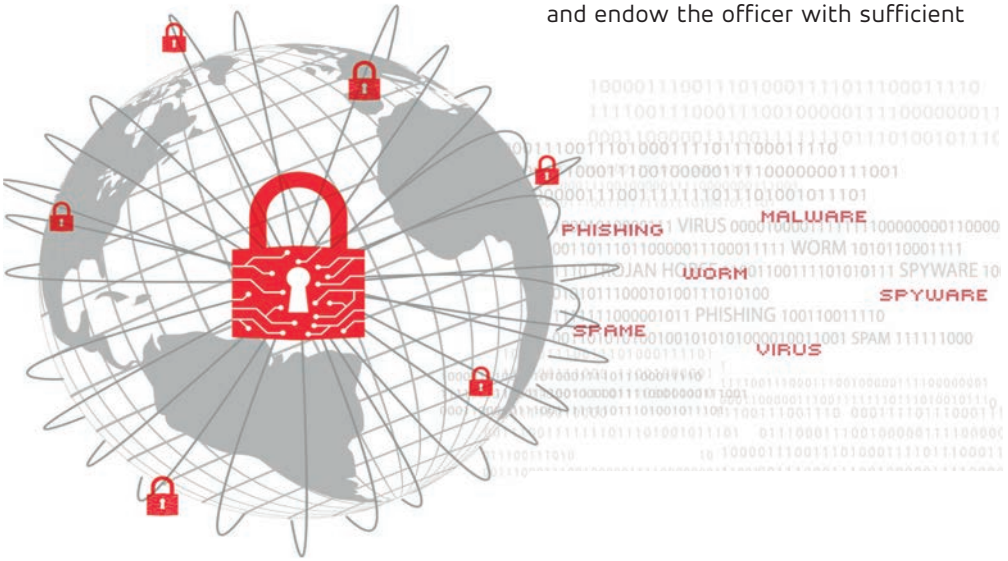
On 28 January the NIS Regulation was approved in Spain. NIS lays down minimum cybersecurity requirements for organizations providing society with critical services. This long-expected regulation brings the EU's NIS Directive into full force within Spain's body of law. Although it refers only to organizations providing critical services, it will in all likelihood be taken up as an across-the-board cybersecurity benchmark.

The NIS Regulation establishes a baseline of minimum cybersecurity measures to be met by organizations, combining measures that are already commonly in place with others that have been taken up only by more cybersecurity-savvy organizations.

The first new development is the obligation for organizations to report any cyber-incidents to the government. This obligation had already been laid down by the GDPR for privacy incidents and is now extended to all cybersecurity incidents. The regulation also brings in the obligation of collaboration between organizations and the government to deal with any incident, blending the organization's own capabilities with the government's coordination in solving the incident and passing on an early warning to other organizations prone to a similar incident.

The second new feature is the government's compliance-oversight capacity by means of communication points between the administration and the organization. It is also endowed with the necessary auditing powers, based on the organization's obligation of reporting its cybersecurity readiness to the government.

The third new feature is organizations' obligation to set up an information security officer as interlocutor with the government and enforcer of the regulation within the organization. The regulation lays down the training and eligibility requirements for this officer as well as the obligation for the organization to input resources and endow the officer with sufficient authoritativeness and independence to be able to fulfil the regulation's responsibilities.



Mariano J. Benito,
CISO of GMV's Secure e-Solutions sector

> The NIS Regulation establishes a baseline of minimum cybersecurity measures to be met by organizations

The minimum measures, for their part, consist of common aspects already well known in cybersecurity: draw up and work with a security policy; apply physical, technical and organizational security measures; set up and follow business-continuity and risk-management plans as well as continuous improvement and cyber-incident-detection and -management plans.

Publication of this regulation brings out the value of GMV's 25+ years of cybersecurity experience and its expertise in providing its clients with the most beneficial services.

Grupo Carreras, cybersecurity in essential sectors during the pandemic

The protection of critical infrastructure and the provision of essential services have become major concerns of countries these days. To address this matter Fundación Borredá organized last November the Congress of Integral Protection of Essential Services and Critical Infrastructure.

It did so with the support of representatives from the Spanish government and the private sector, through its protector partners, including GMV. Over 1000 professionals signed up for the online congress, featuring headline speakers on such subjects as security governance, cybersecurity and the essential services protection model.

As part of the panel "Experiences and applied solutions", GMV talked about its experience with Grupo Carreras on the role of cybersecurity in essential sectors during the pandemic, focusing on the logistics sector.

Javier Ibáñez, CIO and Digital Transformation Leader of Grupo Carreras, and Javier Hidalgo, GMV's Industrial Sector Solutions Architect, presented the joint cybersecurity project of both companies. Ibáñez explained the security role as a crucial feature of the company's digital transformation plan, due to the great amount of information handled; right from the word go, he added, they turned to GMV for the solution.

GMV in particular supports Grupo Carreras in taking stock of cybersecurity in its Computer Emergency Response Team (CERT)'s management project, in cybersecurity training and cybersecurity proselytism. Hidalgo's speech focused on the process set up by Grupo Carreras, viewing cybersecurity from the very start as an across-the-board value with the full involvement of high management and firmly based on a security masterplan, training plan and awareness-raising at corporate level.

GMV adapts ATMs to the maximum security levels of the future

GMV was present at BankSec, the online event organized by Retail Banking Research (RBR) in December 2020 to analyze the characteristics of ATM cyberattacks and recommended the best protection measures against them.

An analysis of the most recent attacks shows that most of the exploited vulnerabilities stem from the use of backdoors by the banks themselves to make their ATMs more user-friendly. For example, the possibility of connecting USBs to ATMs is a weak point that many banks tolerate to enable their technicians to carry out on-site maintenance work.

If we now turn our attention to the ATM networks, we could perhaps define their hallmark trait as stability: stability of the software, of data, transactions and execution in general. We also know that attacks tend to shake up this stability like an earthquake: incomplete transactions, skewed execution sequences, abnormally high or low sums dispensed, etc.

These inherent ATM traits mean that behavior-analysis and anomaly-detection technology really comes into its own here. This needs to be based on stable and well-known system behavior without suffering any upsets caused by vendor- or model-heterogeneity of the ATM networks. The XFS layer provides this desired stability and uniformity, cancelling out the vendor or model idiosyncrasies while also ensuring direct access to the ATM's most critical and basic functions. This layer also allows for a complete and very dependable analysis of ATM behavior, flagging up the slightest anomaly and cutting down the number of false positives.

In many cases, however, the detection of anomalies is not enough to fend off an attack; it needs to be rounded out with measures to block off these anomalies. Once more, the XFS layer constitutes the perfect input point not only for analyzing behavior but also detecting anomalies, taking the necessary measures to ward off this suspicious behavior.

We at GMV have developed a new ATM security product, ***Checker XFS Filtering***. At ATM XFS-level it implements a complete ATM-security solution, combining ATM behavior analysis, anomaly detection and filtering of suspicious actions. This new GMV solution is a natural upgrade of its longstanding ATM-security product, ***Checker ATM Security***, to ensure the maximum levels of security.

Opinion

Man-In-The-Middle cyberattacks in the industrial environment

Information technology takeup in the industrial sphere has been a constant feature in recent decades. An increasing number of companies are now plumping for new information systems in their productive systems with the clear objective of harnessing their competitive edge, such as ensuring production, cutting costs and boosting efficiency. This process, however, as necessary as it is inevitable, does bring new risks into the production systems.

By virtue of its own intrinsic dynamic, security in industrial environments has been geared more towards security through obscurity (STO) than the takeup of security management systems as understood in the information technology sector. Although this STO strategy may have been justifiable in the past, the irruption of information technologies and their ongoing convergence with production systems have inevitably swollen the attackable surface of these systems, bringing in a whole new world where the cybersecurity risk has spiraled.

Luckily, these threats are well known in the conventional IT field and differ little in the specific IoT field in industrial environments, although their development there and the way these threats have to be tackled do call for an environment-specific approach.

Prime among these threats feature those known as Man-in-the-Middle (MITM), where the attack strategy is based on intercepting communications between several IoT devices, falsifying or altering the communications, thereby causing malfunctioning of the productive systems and wrong decisions by operators who have been misled by the false information.

How can we protect ourselves from MITM attacks?

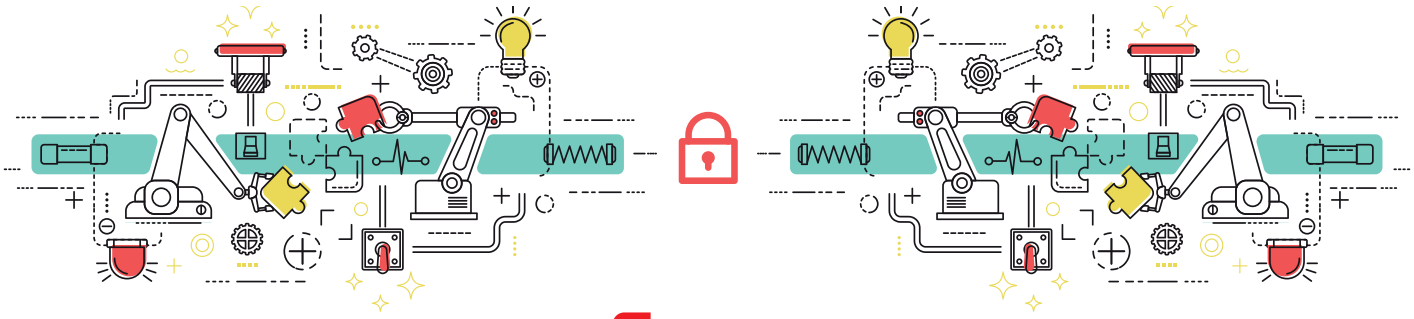
The following bullet points are crucial for protection in an industrial production scenario:

- Establishing design-up security from the start of IoT system rollout rather than tagging it on afterwards.
- End-to-end communication encryption between IoT devices and the management platform, with proper vetting of credentials, preferably based on device certificates.
- Setting up secure connections by VPN when communication with platforms outside the industrial environment is needed.

Javier Hidalgo Sáez.
GMV's Industrial Sector Solutions Architect

An increasing number of companies are now plumping for new information systems in their productive systems with the clear objective of harnessing their competitive edge, such as ensuring production

- End the practice of automatic trust in new devices tagged onto the platform, introducing instead a controlled and programmed device phase-in.
- Instructing employees in the importance of IoT security throughout the whole firm.



How to tackle risks and threats in the digital era

At the end of January the Spanish Certification and Standardization Association AENOR and GMV took part in a conference to debate the new ICT risks, threats and challenges now facing organizations in the digital era, especially in the pandemic we are all now living through. Special stress was laid on the importance of bringing in and certifying new ISOs to lever the necessary levels of security, trustworthiness and resilience for tackling the challenges thrown down by current and future crises, thus ensuring a solid digital transformation in line with business goals.

Boris Delgado, AENOR's Certification Manager, presented the ICT Confidence Platform (*Plataforma de Confianza* TIC) as a solution to the ICT risks of today and tomorrow. This platform forms part of AENOR's Digital Ecosystem, in particular the ICT management and governance model. Its aim is to provide security and confidence ahead of the current and future crises, taking in too the "new normal" with all due guarantees of resilience, continuity and cybersecurity in ICT services and systems. Delgado argued that these international standards are helping organizations cope with the current pandemic, ensuring they can meet their business goals and find out how to fend off new risks, in other words to be sure they're ready not only for today but also tomorrow.

Mariano J. Benito, CISO of GMV 's Secure e-Solutions sector, brought GMV's expertise to the table as a trailblazing firm in the implementation and certification of ISO standards like the new privacy information management standard 27701 . GMV's own response to the coronavirus pandemic was swift, smooth and fleet-footed. Benito explained "GMV had already evaluated similar teleworking and crisis scenarios so we only had to greenlight certain tasks that we already had fully planned and prepared. We had anticipated what we might need and identified and solved any security snags that might crop up". The preventive, sustained and thoroughgoing application of security management systems based on international standards enabled us to take on this situation with complete security and confidence.

One of the latest ISO security standards to be published is ISO27701 on privacy information management systems. GMV was the first to obtain and set up this certification under the aegis of AENOR. ISO27701 meant that GMV was able to implement a company-wide privacy management system based on management systems that were already in place. Mariano Benito highlighted AENOR's role as auditor: "this has turned out to be fundamental as an independent, solid and professional criterion to ensure our privacy management systems were ISO27701 compliant".

GMV, identified as a "Key Innovator" by the European Commission's Innoradar

The European Commission's innovation radar has hailed the technology multinational GMV's developments in natural deformation and 3D handling of medical images

The European Commission's innovation radar *https://www.innoradar.eu* has hailed the technology multinational GMV as a "Key Innovator" on the strength of its developments in natural deformation and 3D handling of medical images, helping surgeons to prepare and plan their work.

GMV's inhouse research has come up trumps again, proving capable of the highly complex achievement of modeling complete relations between anatomical structures and their elastic performance and developing algorithms capable of capturing these complexities, dealing with medical images in near real time.

Carlos Illana, Product Manager of GMV's Secure e-Solutions sector, gives the following account: "Many different aspects of GMV's inhouse R&D under the Rainbow project have been weighed up by the European Commission, praising in particular the deformation simulation algorithms and volumetric medical image segmentation. This helps to solve one of the main challenges of pre-surgery planning, which has hitherto been restricted to bone structures". He goes on: "this groundbreaking innovation would not have been possible without the joint work of highly specialized engineers with trailblazing business expertise too and also worldwide public research bodies".

The European Commission's Innoradar has been set up to identify high potential innovations and innovators in EU-funded research and innovation projects. Its remit is to bring projects to the notice of potential investors, driving the marketing of these developments and the creation of an innovating ecosystem. It is also part of the overarching transparency exercise, to ensure the public at large is kept informed of how EU funds are spent.

The research that has won GMV this recognition is being carried out under the RAINBOW project, the remit of which is to perform research and development into a new generation of practical, user-friendly clinical simulators that are conducive to the design and application of personalized medicine.

Under RAINBOW GMV is helping to develop clinical simulation tools to be applied in procedures of diagnosis, prognosis, monitoring, surgical training, planning, guidance, prosthesis design, implant operations and medical devices. Clinicians will then be able to use this new generation of biomechanical simulation tools directly without needing technical help. RAINBOW is included in the Innovative Training Networks (ITN) of the Horizon 2020 program.

RAINBOW
Rapid Biomechanics Simulation for Personalized Clinical Design
A Marie Skłodowska-Curie European Training Network

Navigation and algorithms: revolution in the operating theaters

The new navigation technology, surgery simulation algorithms and intraoperative imaging have all helped to make surgery more precise and healthcare results more dependable, favoring safety during the actual operation and a quicker recovery afterwards. All this is conducive to a much better patient experience.

In the words of Doctor Marisa Gandía, neurosurgeon of Madrid's Hospital Universitario La Paz, "image-guided surgery represents a true revolution". Navigation technology brought into surgery, in particular, is comparable to what "GPS has meant for the world at large", argues Carlos Illana, GMV's head of product.

In the specific case of minimally invasive surgery, where the surgeons' work is guided by live medical imaging, the technology, based on live displaying of 3D images, allows them to plan and simulate the surgery with intraoperative monitoring. Navigation systems give clinicians an exact idea of the instruments' position and allow them to check the surgical field in a 3D patient image. Computational techniques come into their own here, allowing optimization of the planning in the preoperational phase as well as honing precision and quality of the surgical technique. Under the NAVIPHY project GMV is studying the possibility of offering real-time images and parameters of the surgeons' activity and of any changes that the patients' anatomy might undergo during the operation.

As Carlos Illana points out "surgical navigation systems and simulation applied to minimally invasive surgery are being increasingly taken up during surgical operations because they offer greater safety and precision". Even so, "we want to take this technology up to the next level and improve today's positioning systems while phasing in simulation technology that reduces the need for imaging without forfeiting precision and safety". Work is underway to that end under the NAVIPHY project.

In minimally invasive surgery, as Dr. Gandía explains, a tubular system is positioned by means of neuronavigation and the area to be operated on is established. In such surgery "the tissue is separated by dilatation rather than widespread muscular disinsertion, so access to the surgical bed is much less aggressive". This factor, together with the smaller incision "slashes the infection risk and pain involved, affording a much quicker recovery afterwards. Most patients are back on their feet within 24 hours and get back to work much quicker than after conventional surgery. In short: less pain, damage, bleeding and infection".

GMV is participating in NAVIPHY, a project falling within the Ministry of Science, Research and Universities' research challenges R&D call and subsidized by the European Union (EU) through funds of the European Regional Development Fund (ERDF) project. Its purpose is to achieve greater precision in brain, breast and maxillofacial surgery while also combining them with intraoperative radiotherapy and brachytherapy. It is also looking into new navigation technology, developing simulation algorithms and weighing up the use of various intraoperative imaging technologies.

GMV participates in ProPatiens's Telemedicine Healthcare publication

A total of 29.5% of chronic patients used telemedicine during the COVID-19 lockdown. Takeup was higher among women (32.7%) than men (25.3%). These are the findings of the study "Lockdown internet use by patients and clinicians for online consultations (*Uso de internet durante el confinamiento para consultas no presenciales con su médico o profesional sanitario que le atiende*), drawn up with GMV's collaboration by the ProPatiens Institute and recorded in the free e-book Online healthcare (*Asistencia sanitaria no presencial*). Much of GMV's collaboration was based on its tried and tested telemedicine platform ***Antari***.

The keynote interview of Carlos Royo, manager of GMV's Healthcare Strategy and President of the Digital Healthcare Committee of the Spanish Association of ICT Companies (*Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones y Contenidos Digitales*: AMETIC) stresses "the urgent need to bring in a digital transformation of the national health system, not only to make sure it is sustainable into the future but also to empower citizens to make their own informed decisions on what is best for their health, obviously under the guidance of healthcare professionals".

GMV features among the intraoperative radiotherapy TOP 10

According to the latest worldwide market research carried out by Apex Market Research, the technology multinational GMV ranks as an innovating firm among the intraoperative radiation therapy (IORT) Top 10. The companies included in this Apex Market Research ranking are those whose products have displayed substantial innovations in comparison to their competitors.

IORT is a high precision method of administering during the surgery itself a single, targeted high-radiotherapy dose to the tumor bed/microscopic residue or, in the case of unresectable tumors, to the macroscopic tumor. This single dose is targeted directly at the bed to be irradiated without affecting the surrounding healthy tissue.

The growth of the global IORT market is being driven by 3 main factors: the rising incidence of cancer, technological advances and the advantages offered by IORT applications. Apex's study shows that the IORT market will add up to 67.8 million dollars by 2024, with a CAGR of 7% from 2019 to 2024.

GMV boasts the world's only radiosurgery planner ***Radiance™***, which improves IORT safety, giving clinicians a complete analysis of the patient beforehand. This enables them to make crucial decisions before the surgery itself, identifying the optimum treatment adapted to suit each particular case (personalized, translational medicine).

GMV ranks among the worldwide leaders on the strength of its inhouse IORT planner called ***Radiance™*** and its commercial alliances with other market leaders like Carl Zeiss, Meditec AG (Germany) and IntraOp Medical Corporation (USA). This groundbreaking software provides all necessary data for previous documentation of the surgery to be carried out, calculating the exact parameters to be applied by the clinician in the operating theater before going ahead with the surgery. It also provides high-quality multiplanar (MPR) images and a 3D view of the patient, allowing a simulated display beforehand of the treatment results.

Technology for sharing healthcare-research and -management knowledge

GMV's inhouse development ***uTile PET*** (Privacy-Enhancing Technologies) enables hospitals, research centers and the pharmaceutical industry to share their knowledge without exposing patient data to any risk of disclosure or even moving it from its site of origin. Advanced cryptographic methods keep the data encrypted while all necessary calculations are made to improve the precision of AI techniques and ensure 100% data anonymization.

This is a crucial breakthrough to deal with the particular privacy constraints of healthcare management.

Because of these particular difficulties, healthcare management data tends to get backed up in so-called data silos. Patchy national and cross-border legislation then prevents this scattered information from being pooled and brought together. ***uTile PET*** gets round this bottleneck, freeing up such crucial information as biomarkers, prognoses, average patient age, clinical treatment, etc, without jeopardizing patient data privacy.

uTile allows healthcare professionals to strike the right balance between data privacy and data harnessing. The data remains encrypted throughout the whole computation process, whether on-premise or cloud hosted, fully protecting patient privacy.

GMV supplies Jerusalem light rail's AVLS and DMS

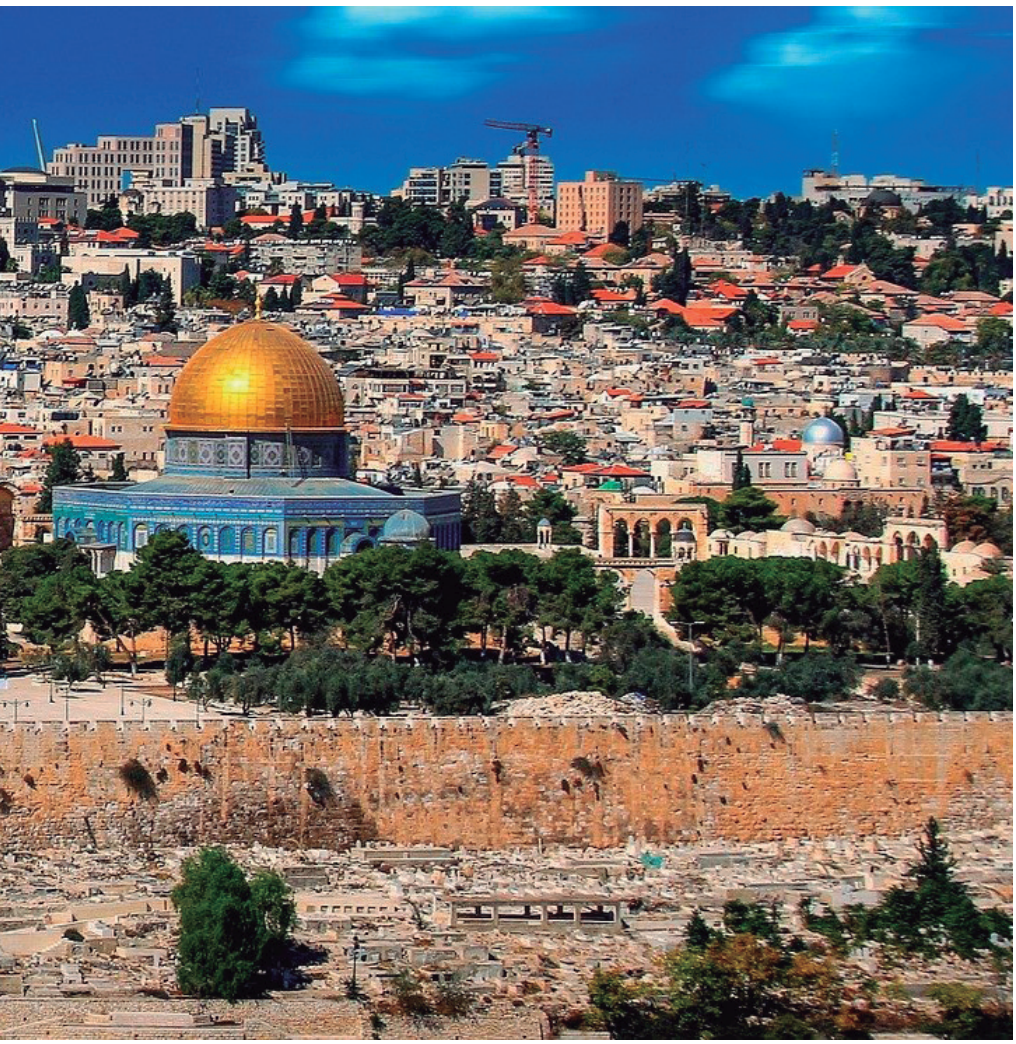
GMV's solution for Jerusalem's light rail will be based on its inhouse railway and tram fleet management system ***SAE-R®***

GMV has recently been chosen by CAF group for supply of the Automatic Vehicle Location System (AVLS) and Depot Management System (DMS) for its light-rail project in the Israeli city of Jerusalem. This project takes in not only the extension of the red line, currently in operation and now to be run wholly by CAF, but also the new construction of an additional line, the green line.

The global 4½-year project, to be performed by the consortium made up by CAF and the Israeli construction firm Saphir, takes in 160 trains (46 from the red line, which will be reformed, plus 114 from the new line), 76 stations and 3 depots.

GMV's solution for Jerusalem's light rail will be based on its inhouse railway and tram fleet management system ***SAE-R®***, already taken up in projects like the communications platform for the railway operators RENFE in Spain and ONCF in Morocco as well as the tramlines in Sydney (Australia), Warsaw (Poland), Kaohsiung (Taiwan) and Zaragoza (Spain).

The ***SAE-R*** to be set up in this case will feature the traditional functions assigned to systems of this type, such as precise fleet tracking (both on a geographical map and detailed synoptic maps of lines and depots), radio communications and messaging management (both with drivers and users with fixed and portable radios) information for passengers onboard and in the station (including definition of contents and playlists), driver management (control of rosters and shifts) and the most advanced service regulation operations for dealing with



any unforeseen event plus real-time monitoring of alarms and states of both own and external systems.

These functions will be combined with other advanced upgrades such as automatic train operation in aspects such as dynamic route establishment, crossway priority requests, flange lubrication, door opening, tunnel lighting, control of bicycle storage space or telecommand from the control center of certain vehicle comfort parameters (air conditioning, volume control in passenger information equipment, control of onboard lighting levels, etc).

One of the ***SAE-R***'s built-in modules is the Depot Management System (DMS), run from the same user applications as the AVLS module to ensure more efficient operation. The DMS module's main function will be rolling-stock management (line entrances and exits) and track occupancy in the various depots. All this will be based on a set of track occupancy policies to be defined by the operating firm and real-time monitoring of the state of the signaling system installed in depots (signals, points, axle counters, track circuits ...).

GMV's fleet management system will be installed in a multi-system environment in which it will be integrated functionally with a host of external systems both in the control center (SCADA, CTC, RADIO LTE, CMMS, Scheduling Tool, Ministry of Transport [MOT] ...) and onboard (TCMS, Radio LTE, Route Request System [RRS], Traffic Priority System [TPS], ATP, Passenger Counting System [PCS], CCTV, Ticketing, etc). Implementation of these interfaces, barring exceptional cases, will be based on communication standards such as BUS NAOS, TRDP and SIRI.

All the trains will be fitted with GMV's inhouse onboard units and touchscreens in both cabs plus driver HMI.

The onboard technology will be rounded out with the installation of a control center in the central offices comprising a set of servers in a virtualized environment and a series of workstations that will allow the line operator to ensure smooth service operation. It will also work both on- and offline; the latter is then made available to external systems for calculating system-operation KPI values.

Both at control center and onboard level the ***SAE-R*** will be set up on a failover redundancy basis, ensuring high system availability in the event of any one-off component errors.

Again, at both control-center and onboard level the ***SAE-R***® will also feature the most advanced cybersecurity techniques, the whole system being submitted to a cybersecurity vulnerability analysis by a specialist external firm.

GMV responsible for Castilla y León's demand-response system

Last January GMV was yet again awarded the contract for running and maintaining Castilla y León's demand-response system. The contract this time will run for two years with a possible 23-month extension.

The demand-response system offers an efficient transport system for rural zones with a scattered, low-density population, such as Castilla y León.

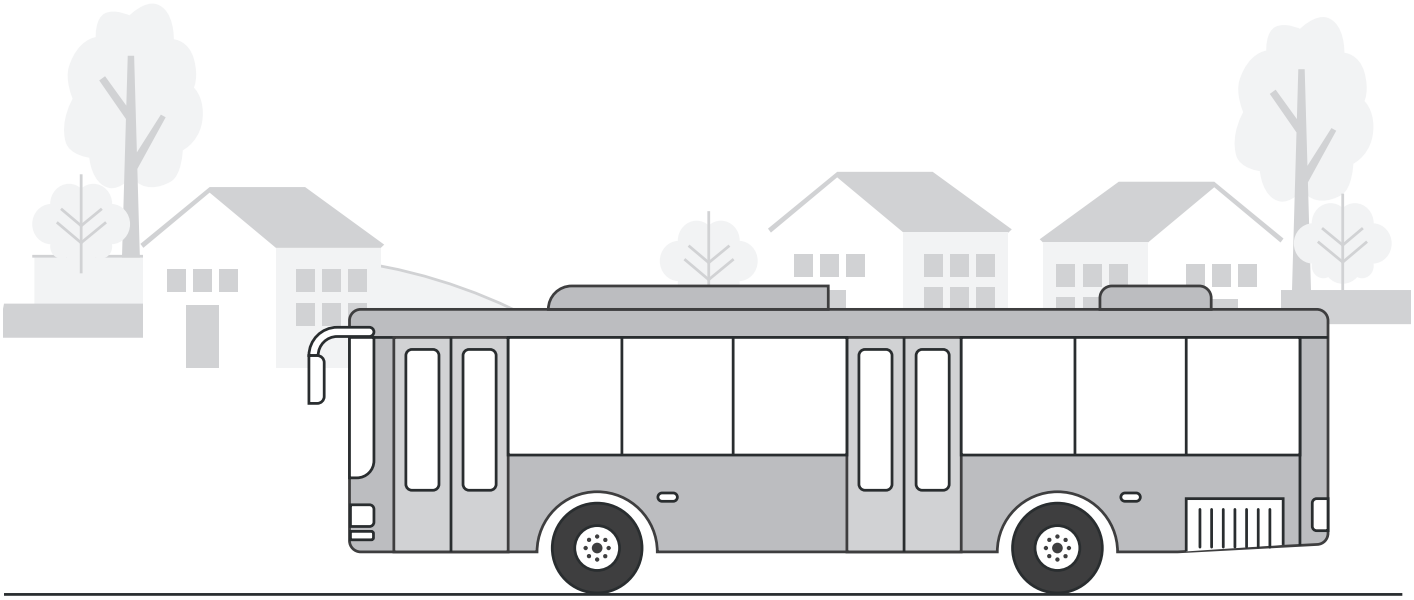
Under this mode of transport buses run only to those places where the service has been booked. This means less mileage, less energy expenditure and lower environmental pollution, in short, a cheaper, more efficient and ecofriendly service.

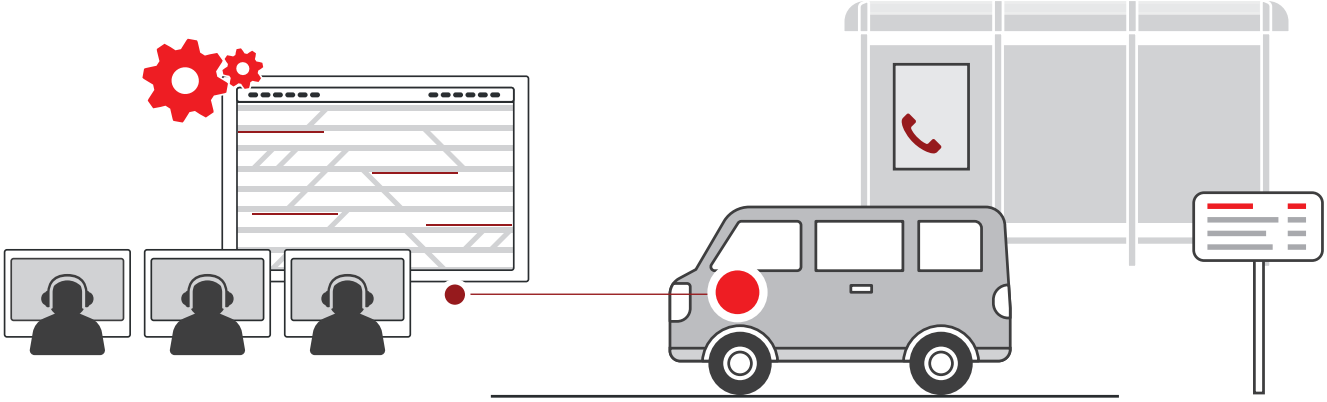
Castilla y León's booking center, located on GMV's site in the technology park called Parque Tecnológico de Boecillo, in Valladolid, will be staffed with more employees and backup during the summer months when transport use in rural areas is much higher. A new quality system in the call-recording system will favor higher visibility in identification and measurement of service quality.

The central service-booking platform runs a 327-bus fleet and caters for one million inhabitants, 5015 sites, 123 operating areas and 1944 service routes. It also deals with a yearly average of about 250,000 journeys.

Up to now service bookings could be made only by phone, calling a free number. Project renewal now envisages setting up a responsive user website where anyone can make the request by cellphone. They can also check information on routes or see informative messages, among other functions.

This contract renewal consolidates GMV's reputation as the most experienced demand-response provider in Spain. This is borne out by the 17 years of work in the demand response sector, building up a fine-tuned knowledge of design, commissioning and maintenance of this type of ITS in the rural world.





GMV to supply the fleet-management and ticketing systems for all Vectalia's buses

Vectalia has turned to GMV for supply of the fleet-management and fare-collection systems in its first concession award within the first block of concessions put out to tender by the Regional Authority of Galicia (*Xunta de Galicia*).

This new project with Vectalia puts GMV in pole position for Galicia's ongoing renewal of transport concessions and marks it out as a benchmark technology provider of this and other concession firms operating in the region.

The Xunta de Galicia is now in the process of renewing its transport concessions throughout the whole region. To do so, it has held two public tenders in which Galicia's operating companies will renew or obtain new 10-year concessions.

Under this umbrella Vectalia has taken up GMV's advanced fleet-management and fare-collection systems not only for its first 16 buses belonging to the concession awarded within the first block to be put out to tender by the Xunta de Galicia, but also the 51 buses awarded in the second block, providing a service up to the end of 2020.

In technical terms GMV will be fitting Vectalia's buses with a ticket vending machine to work with the *Xunta de Galicia's* contactless farecards, incorporating too EMV payment technology and a QR code reader, fitting it out for use as an onboard fleet-management system.

At control-center level the company will also be supplying its ticketing and fleet-management backoffice systems to pass on fleet-running information to the *Xunta de Galicia's* central systems.

ALSA once again contracts GMV's fare payment system for Almería

Back in November 2018 GMV was chosen by ALSA to modernize the ticketing system of the buses running on Almeria's urban transport system. Now ALSA and the Almeria Transport Consortium (*Consorcio de Transportes del Área de Almería*: CTAL) have once more turned to GMV for updating the electronic fare collection system installed by the company in 2001.

The new contract includes supply of onboard ***ETC606i-8*** ticket vending machines for the 60-bus fleet. These cater for the sale of single-journey tickets plus validation of the current farecard of ALSA's subsidiary, SURBUS, and the farecards Mifare Classic and the new Desfire of the Andalusian Transport Consortium (*Red de Consorcios de Transporte Andaluces*: RCTA).

The vending machine will be fitted with a GPS receiver and built-in 3G modem. A router already installed by ALSA will be used, however, so that all communications can be managed from a single SIM. The GPS receiver will enable positioning data to be brought into relation with validations, this information then to be sent on in real time to CTAL and kept in ALSA's central system. The equipment will also automatically pass on from one stop to another to ensure proper recording of the passenger boarding stop.

Recharging for SURBUS's own farecards will be managed onboard the buses by means of 3 ***ETC606i-8*** machines installed in SURBUS's customer attention office.

The contract also takes in 6 inspection terminals in ruggedized (shock resistant) smartphone format for managing inspection of the SURBUS and RCTA farecards. A mobile printer is also issued for dealing with any fraud situations and giving fines on the spot.

The central system includes system-configuration and data-processing applications and also gives a set of transport-management reports plus an application for exporting sales data to ALSA's own applications.

GMV will supply the system in the following months for the system to come into operation before the end of 2021.

GMV implements its account based ticketing for the public transport in Malta

Malta as a country relies heavily on its tourism business so its fare systems need to be top-notch. With this in mind, CONCESIONES UNIFICADAS has turned to GMV for implementing Malta public-transport's account based ticketing (ABT) system.

GMV has been running its in-house ITS system in Malta for the last 6 years, including its all-in fleet-management, fare-collection system (card based system), passenger-information and onboard video-surveillance system for the 400+ fleet.

ABT will enable new fare policies to be phased in quickly and rules to be transferred between different means of transport, etc. at back office level without affecting any development at onboard level.

ABT is easy to maintain; fare logic is managed and calculated/ processed at back office level instead of the onboard level (i.e. no logic on the onboard level). This means the system can be updated quickly from a central location and is able to keep up with the pace of technology. In comparison with this low-maintenance ABT system, working with a single back office, an entire network of locally-hosted equipment is extremely high maintenance.

The travel entitlement in the ABT system is a passenger token.

GMV will be able to graft this ABT system onto the currently installed equipment. This project includes overall Fare Collection System software development at onboard and Back office level. The pilot scheme will be launched in six months, after which the current tradition card based system will be migrated into ABT. For example, the passenger card will act as a token without needing to replace the card.

GMV wins follow-on Poland's FMS and PIS maintenance agreements

At the end of 2020, GMV concluded its third consecutive post-warranty system servicing agreement. Under this agreement, in 2021 GMV maintains the Fleet Management and Passenger Information System within the scope of central software, onboard units in 437 vehicles and 93 LED panels at the stops.

The agreement also covers the complete electronic ticketing system with the central software, 36 stationary ticket vending machines supporting cash and cashless NFC and EMV payments, 317 mobile ticket vending machines supporting cash and cashless NFC and EMV payments as well as 1,679 onboard NFC validators. In addition, other subsystems, such as the onboard CCTV video surveillance system with 1,165 cameras or the automatic passenger counting system, are also covered by GMV's maintenance.

The largest collective transport system in Poland functions in Warsaw, where GMV also provides maintenance services. Under an agreement concluded with Warsaw Trams, the country's biggest tram carrier, in 2021 GMV is responsible for the maintenance of onboard geolocators in 530 trams plus the provision of vehicle GPS position data to the Purchaser's control centers.

These systems are constantly extended with new elements, such as panels at the stops, and periodically covered by maintenance agreements. Under newly concluded agreements, in 2021 GMV provides the Municipal Roads and Public Transport Authority with the services related to the upkeep and maintenance of the server infrastructure together with the central software of the FMS, 125 LCD panels at the stops and GPS onboard units in 325 public transport buses and trams.

In Toruń GMV carries out post-warranty upkeep and maintenance of the tram system launched in 2014. In 2021, the service is provided on the basis of another maintenance agreement concluded at the end of 2020 and covers comprehensive servicing of all elements of the Central Fleet Management and Dynamic Passenger Information System, including FMS central software, onboard units in 51 trams and 67 LED panels at the stops.

Commissioning of the new serial CCTV of Barcelona's Metro trains

GMV has successfully completed implementation of the onboard video-surveillance system of the 47 series 5000 and 6000 trains of Metro de Barcelona, and in the 10 trains of the new series 5000 and 6000 trains to be supplied by CAF to TMB.

The project scope includes the deployment on each train on an onboard multiservice ring-configuration Ethernet with one switch per car, which caters not only for the new CCTV system but any other to be phased in in the future.

An inhouse GMV network video recorder (NVR) has also been supplied, capable of recording images in Full HD format with simultaneous video playback and exporting. Two NVRs per train have been fitted in redundant mode. In the event of failover the active NVR will automatically and autonomously take on recording of all cameras.

The system has been fitted with communication concentrating nodes, which are responsible for managing all onboard information, whether coming from the video surveillance system or elsewhere, while also making it available to ground through the wireless communication channels best suited to the train's location and available cover. For this purpose it is enabled with WIFI and 4G/LTE connectivity.

The system is then rounded out with IP cameras and cab-mounted IP cameras with infrared in the new CAF trains plus analog-digital codifiers for reuse of the analog cameras fitted in some trains.

A centralized video-surveillance server has also been fitted plus operator posts in the metro control centers and security centers plus civil protection on Sagrera base.

The Urban Air project for sustainable mobility in Valladolid comes to an end

Urban Air

Interreg
España - Portugal
Fondo Europeo de Desarrollo Regional
Fundo Europeu de Desenvolvimento Regional
UNIÓN EUROPEA
UNIÃO EUROPEIA

The Urban Air project is part of the Interreg initiatives for cross-border cooperation between Spain and Portugal. Led by Valladolid University, the project seeks to develop mobility proposals with special stress on shared bicycle use. To assess the reduction in the carbon footprint associated with the rollout of this system, a series of sensors were fitted to the bikes to measure air quality along the cyclists' routes.

Under this project GMV has developed a mobile app controlling shared bike use by means of smart Bluetooth-communicating bike locks to give users access to the bikes.

The application enables the bike trips to be monitored by telephone connection with the fitted sensors. The cyclists can therefore record air quality along their habitual commuting routes and quantify the reduction in emissions achieved by using a bike instead of a car for commuting.

The pandemic threw a spanner into the works, since it is not possible to guarantee bike disinfection between each use. For some months, therefore, the shared bike use system had to be changed into a lending system whereby each user was allocated a bike for a given period of time.

GMV adapted the bike loan system so that it would work in terms of personalized allocation. The loan service is now up and running in Valladolid University with 50 bikes, and arrangements are already being made for the next academic year.

Course on pay-as-you-go ITS

In early March GMV took part in a hybrid, online-onsite event under the title "Course on ITS for pay-as-you-go road use", organized by ITS España and coordinated by ARUP.

Carlos Barredo, head of GMV's Automotive R&D and Aftermarket division, spoke on behalf of the company about the satellite-technology systems the company is currently working on. He described the concept and architecture of these systems, their various components including the back-office platform, communication systems, enforcement subsystem and the onboard unit, OBU.

Barredo also described GMV's expertise in pay-as-you-go road-use systems based on GNSS technology and its range of solutions, especially the smartphone as user enabler and toll-payment technology. Architecture of this type, he added, could be expanded to the management of low-emission zones in cities.

Last but not least he illustrated this with some success stories and also brought out the synergies existing between cooperative intelligent transportation system (C-ITS) services and the vehicle's other connected services.

TachograAPP, the European Commission's safe-transport study, is brought to completion

GMV has drawn up a study offering a compilation of possible solutions integrating satellite positioning and communications technology to find out how to apply them in freight- and passenger-vehicle monitoring

The TachograAPP study, financed by the Directorate General of Mobility and Transport (DG-MOVE), coordinated by VVA and led by GMV in terms of technical analysis, has been brought to completion. The study's remit was to analyze the possibility of using a smartphone as tachograph on the way towards a smart tachograph.

Under the regulation in force since June 2019, all freight vehicles weighing over 3.5 tons or passenger vehicles carrying more than 9 people must be fitted with a smart tachograph. This device records vehicle activity to ensure it complies with driving and driver-rest times, with the overarching aim of minimizing the number of fatigue-caused road accidents.

During routine checks, however, the authorities detected many cases of fraud. Fudging rest times obviously has an economic advantage because the vehicle can fit in more trips, but the risk posed to the driver him/herself and other road users is high.

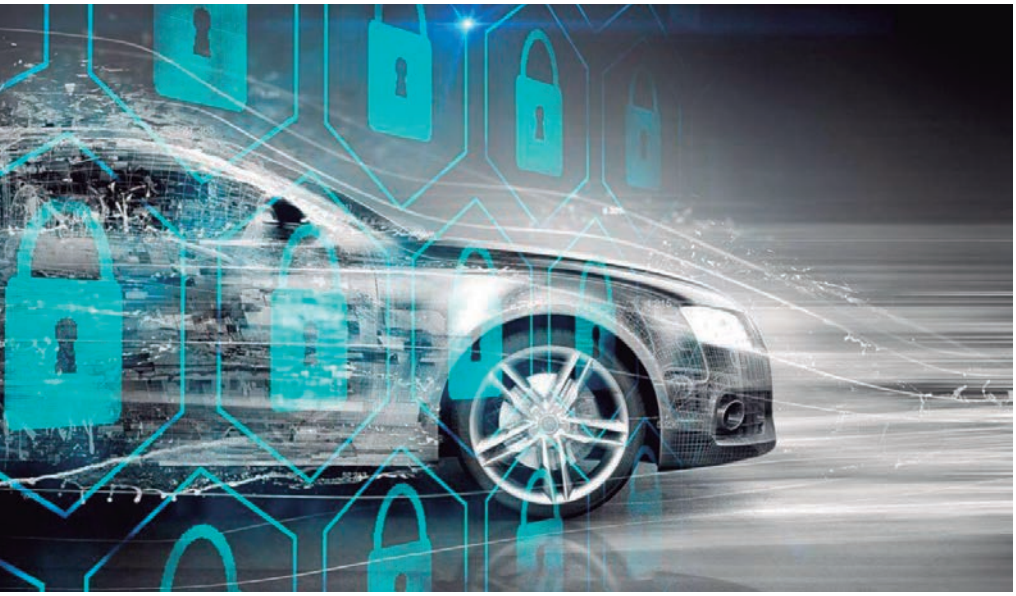
To improve road safety for everyone, head off fraud and fight the mafias that modify and override the current tachographs, the European Commission is looking into the latest breakthroughs in communications technology, sensors, satellite positioning, biometric authentication and IT security.

GMV's study offers DG-MOVE a compilation of possible solutions integrating this new technology to find out how to apply it in the monitoring of freight and passenger vehicles. This helps to tighten control over vehicle activity and preserves or improves the level of safety offered by today's solution (EAL 4+).

The analysis has confirmed the feasibility of combining this vehicle technology and cloud data analysis. This would allow traffic authorities to detect any infractions in real time, communicate remotely with each other and exchange information with vehicles showing unusual conditions.

It would also reduce the workload of agents in charge of road checks and enable the driving conditions of a higher number of vehicles to be monitored simultaneously. This would reduce road fraud and cut down the number of fatigue-caused road accidents.

GMV's vehicle cybersecurity work continues apace



The cybersecurity of connected and autonomous vehicles is one of the hottest topics in the automotive community, especially with the new cybersecurity regulations like UNECE WP.29 and ISO-21434.

For some years now GMV has been working on new security protection techniques for vehicle communication with constant upgrades as the situation changes.

To meet the new threats and challenges GMV is pursuing its new automotive cybersecurity project, upgrading its IDPS model for connected and autonomous vehicles and looking into new solutions to make V2X connectivity more robust.

One of GMV's prime objectives for 2021 is the rollout of a vehicle-intrusion detection system based on real-time AI algorithms (AI-IDS).

The project's main remit is to upgrade our AI-IDS in order to provide a deterministic, highly-configurable, rule-based system incorporating deep-learning technology for access-control and authentication in all vehicle communications and interfaces. The project also includes a component to increase the scope of vehicle-infrastructure (V2X) communications.

The vehicular public key infrastructure (VPKI) is catching on as the go-to solution for managing V2X communication credentials. This project poses a study to pinpoint all VPKI limitations and scalability and interoperability weaknesses while also putting forward new V2X communication credential management solutions.

The aim is to improve execution time security, privacy and trustworthiness of the devices, using a scalable and decentralized system that avoids the need for complex infrastructure like the PKI.

The first results show that GMV's input in all this new architecture could be a part of the connected and autonomous vehicle's future, highly appreciated by our clients, both OEMs and TIER I suppliers.

GMV participates in the webinar of the Madrid pilot deployed in the C-ROADS project

On 4 February GMV participated in the webinar of the Madrid pilot deployed in the C-ROADS project, organized by ITS España. The webinar presented the main deployment data and dealt with salient aspects being tackled thanks to the participation of all stakeholders.

GMV is supplier of the On-Board Units (OBUs) and also provides the data-analysis organization with a website showing logs of both the OBUs and the HMI. Other types of data are also recorded such as messages received in the OBUs from the Roadside Units (RSUs) and navigation logs.

GMV presented the vehicle OBUs and the role they play in C-ITS architecture, based on V2X communications. An explanation was given of the interaction of these key parts of C ITS deployment with the rest of the roadside components, plus the role played by the HMI and GMV's server, which receives information from sources like the DGT 3.0 platform and MC30.

Various examples of the smartphone app user interface were also shown for diverse use cases of Day 1, Day 1.5 services and hybrid communication services, with the aim of improving the driving performance and thereby enhancing the safety of drivers themselves and hence other road users.

Lastly, the vehicle management website was also displayed plus the data recording website deployed by GMV, with an explanation of its diverse features.

GMV collaborates in use case certification of the DGT3.0 platform

The DGT 3.0 connected vehicle platform is an initiative of the Spanish Traffic Authority (Dirección General de Tráfico: DGT) to facilitate real-time data exchange between all mobility stakeholders in pursuit of Vision Cero: 0 deaths, 0 injuries, 0 congestion and 0 emissions.

GMV is working hard on cooperative systems as part of a drive towards a smarter, more sustainable and safer mobility to reduce the accident risk on all Spain's roads.

Under the European C-ROADS project GMV has developed a smartphone app that works as human-machine interface (HMI) for the On-Board Units (OBU) and also taps into the DGT3.0 pilot to inform users of any upcoming event on their route to improve their driving decisions. The app is both iOS- and Android-enabled.

In 2020 the app was successfully integrated with the DGT 3.0 platform in terms of scheduled roadworks and incidents. The certification of scheduled roadworks use cases showed that the smartphone app received information from the DGT3.0 platform and notified the user about upcoming roadworks. The driver then changed lane and cut down his or her speed smoothly without the need for any last-minute changes.

Certification of the incident use-case showed that receipt of information from DGT's Traffic Management Center allowed drivers to react smoothly and beforehand to a vehicle halted on the road.

The scheduled roadwork and incident use cases can now be added to the list of Virtual Message (VMP) and V-16 signal use cases already deployed and integrated beforehand.

GMV will continue with the integration of the DGT 3.0 connected vehicle platform as our services become available while also continuing to work on and develop this advanced technology in the interests of sustainable mobility and improved road safety.

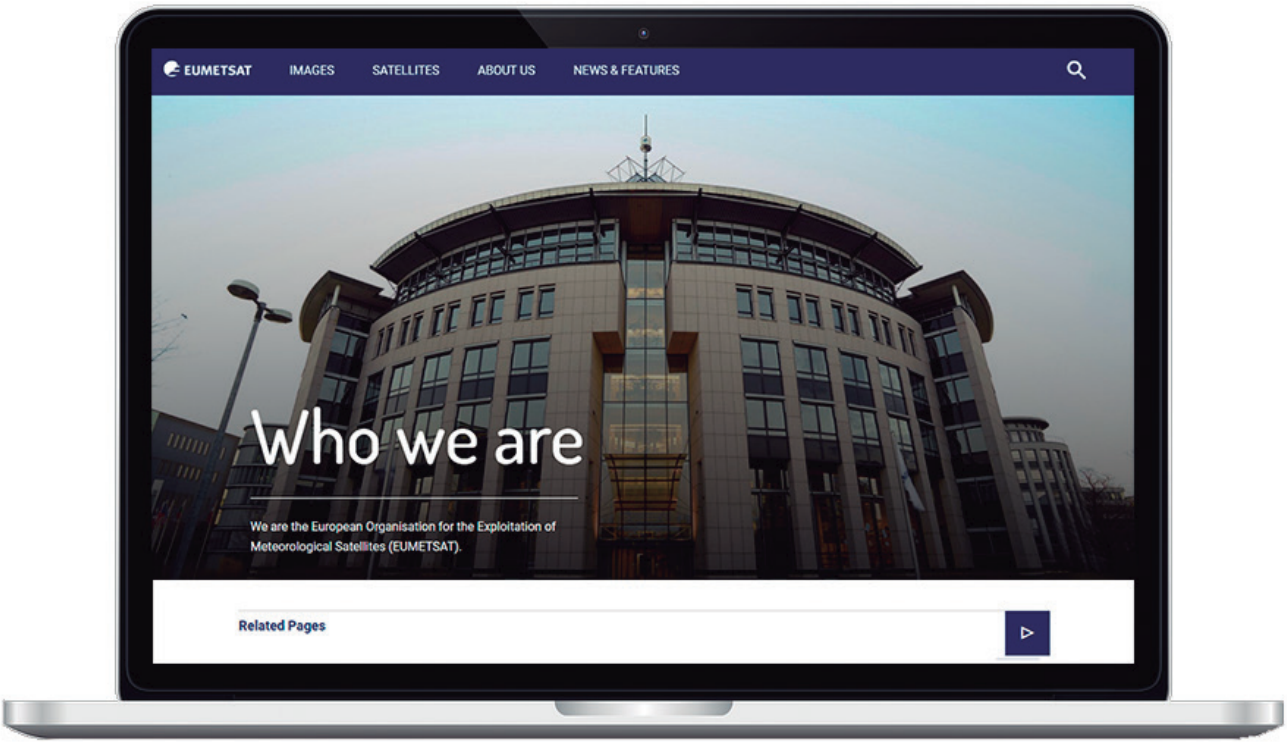
GMV sets up EUMETSAT's new website

EUMETSAT, the European operational satellite agency for monitoring weather, climate and the environment from space, has overhauled its website, using the latest, cutting-edge development trends and the most advanced cybersecurity services, doing so with GMV's collaboration.

GMV has drawn on its longstanding expertise in all the technological skills required for carrying out a project of this type (web development, hosting, engineering, managed services and incident response) to set up a more integrated, easier-to-manage and higher-quality website. After more than ten years of collaboration in other EUMETSAT activities and units, GMV has built up a profound knowledge of EUTMETSAT, its procedures and infrastructure.

The new website, as developed and commissioned by GMV, upgrades the old web portal architecture into a state-of-the-art contents manager. Fully hosted in the cloud of Amazon Web Services (AWS), it thus benefits from all the capabilities of a self-scalable and highly reliable site, cutting down running- and maintenance-costs and minimizing updating- or maintenance-downtime. It taps into AWS's CloudFront content delivery network to boost performance, trimming response times to the bone.

The new website thus brings in improvements in continuity, contingency, scalability and flexibility. One of the crucial aspects here is the provision of cybersecurity services. For this reason the new site is monitored by GMV-CERT, which acts too as an incident response center. This guarantees the necessary cybersecurity level for installations of this type.



Opinion

Cloud Computing in times of pandemic

Cloud takeup in Spain continues to rise steadily. According to IDC Research Spain's report "Multicloud Solutions for the Digital Transformation" 40% of the main IT expenditure in 2022 was cloud related. An increasing number of companies are tending towards this model, transporting part of their systems, initially the least critical, to phase in increasingly critical services from there on.

Europe is now driving initiatives like "EU Federations of Cloud" or "GAIA-X". Spain is pretty well positioned here, and the major cloud providers are now expected to up their profile continually in the national territory.

COVID-19's knock-on effects on cloud computing

This crisis has brought in a series of changes and thrown up new constraints that have accelerated cloud takeup even more, mainly due to its flexibility and autonomy. Just as the 9/11 terrorist attacks nearly two decades ago spawned a flush of backup centers and contingency plans, today's COVID-19 pandemic has brought out the importance of flexibility and system dispersion capacity, driven by the need to set up teleworking systems on a mass scale and skirt the traveling constraints.

Doubts about cloud safety, however, linger on, especially in terms of data confidentiality. A number of questions are begged. Who can access my data? Are there any risky backdoors? Can my data be sent to certain countries? It is therefore crucial for our systems to be underpinned by proper security measures: Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), data encryption, Identity and Access Management (IAM), etc.

Present and future of cloud models

Within the digital transformation process many firms are taking up the best-suited cloud model in each case. In general this is the hybrid model, where the most important assets would be kept in the on-premise datacenter and the rest in the public cloud.

The main advantage of this model is to be able to tap into the public cloud to cater for peaks and new needs without depending exclusively on the cloud. On-premise infrastructure can also be used more efficiently since there no longer has to be spare capacity to cater for peak times. From the security point of view, the hybrid model reduces risks considerably, providing the right balance is always struck between the systems rolled out on premise and those hosted in the cloud.

The current trend is towards multi-cloud solutions, allowing deployment in several clouds, moving content seamlessly from one to another to improve the service, cut costs and minimize risks. It is vital for the design to be cloud agnostic, avoiding dependence on the specific services of one particular cloud provider, otherwise it might prove difficult to leave this cloud or move contents between several public clouds. It should be borne in mind too that improper movement between public clouds can lead to fines, so it is crucial to design the system with expert advice.

Antonio Cabañas
Manager of GMV's Cybersecurity and Infrastructure Division

This crisis has brought in a series of changes and thrown up new constraints that have accelerated cloud takeup even more, mainly due to its flexibility and autonomy

GMV collaborates in enerTIC's 9th Smart Energy Reference Guide

For yet another year GMV has collaborated in the Smart Energy Reference Guide. The 9th in the series bears the suffix "Technology for improving energy efficiency" (Guía de Referencia Smart Energy "Tecnología para la mejora de la Eficiencia Energética). Under the title "Good practices, solutions, 100 fundamental providers and trends in 2020", the guide, drawn up by the enerTIC Platform, gives a wide-ranging picture of the potential of technology transformation in the field of energy efficiency and sustainability.

This year's guide looks closely at the impact of digital transformation as a major phenomenon in today's society, stressing the boosting of competitiveness and sustainability on the strength of new technology trends, with sights set on achieving the Sustainable Development Goals by 2030.

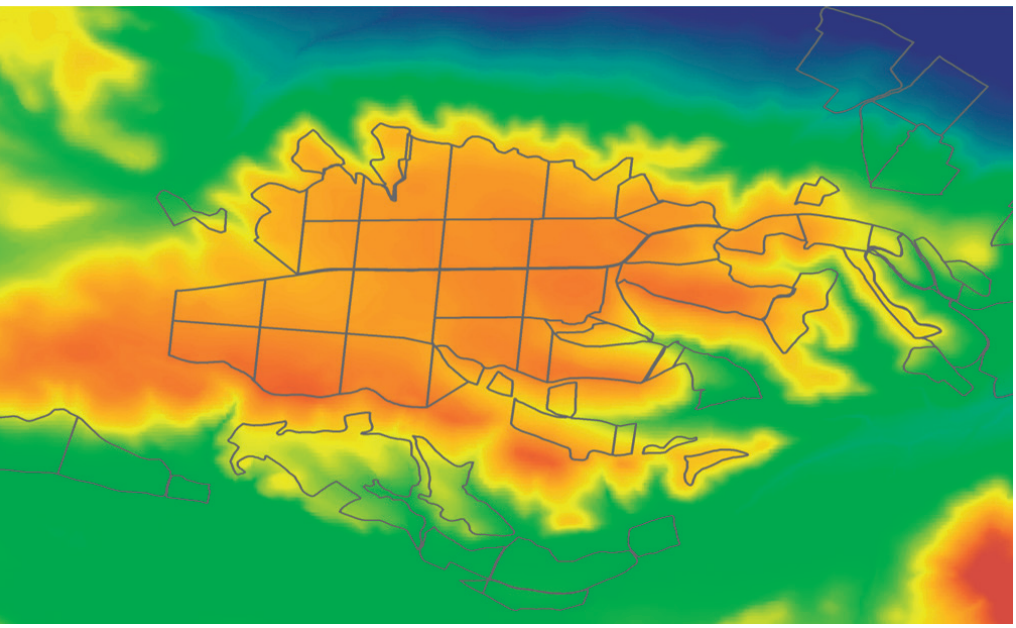
The guide identifies 2021 trends, drawing on the knowledge of experts from the enerTIC platform. Miguel Hormigo, Industry Manager of GMV's Secure e-Solutions sector, stressed the importance of immersive systems to change traditional teleworking systems, improve telecommunications to boost quality and user experience, intelligent sensorization for IoT-based decision-making and hyperautomation, i.e., the quest for intelligent automation (Robotics and AI) of any improvable process to reduce human presence in working environments.

The guide is a key document for executives leading technology strategies, innovation, operations and sustainability to find out the latest breakthroughs and technological solutions with the biggest impact on competitiveness and efficiency.

Innovation and digitalization, two drivers of today's agriculture

Innovation, digitalization and sustainability are all set to be key features of future farming. We have to be able to change our ways of farming, tapping into technology and harnessing all available data, in other words, farm smartly.

GMV's third-day speech at AgroExpo, a meeting point for the farming sector organized by the Tradefair Institution of Extremadura (Institución Ferial de Extremadura: FEVAL), centered on innovation and the phasing in of new technology as the mainstays of smart farming. First up, Miguel Hormigo, Industry Manager talked about the smart farming solutions GMV has been working on recently: AI to classify images, operational and predictive maintenance, sensor development and integration of IoT networks for traceability and specific needs, process automation and robotics, etc.



Next up, Antonio Tabasco, head of remote-sensing and geospatial analysis, focused on Wineo as a fine example, the advanced geospatial data analysis service to support decision-making in agriculture. Wineo processes and integrates data from many different sources (agro-climatic data, satellite images and IoT sensor technology) using an advanced data-based, crop-modeling, machine-learning strategy. This provides a field-analysis smart layer to support design of fertilizer campaigns, crop-growth monitoring, irrigation recommendations and precise yield estimates, plus decision-making based on objective data.

GMV establishes a permanent Brussels Office

The office will work in close collaboration with EU institutions, in particular the European Commission, the Council of the European Union, the European Parliament and the EU agencies

GMV, boasting a strong EU footprint and established companies in seven member states, has now become the sixth biggest space employer among the large industrial groups. To match this growth, the company has set up a permanent Brussels office to reinforce the dialog with the EU and to enable a continuous and constructive communication with the various institutions and stakeholders, doing so with the aim of shaping and implementing the EU agenda, and addressing the important challenges and opportunities of GMV's main business activities today: Space, Defence, IT and Transportation.

GMV's Brussels office will work in close cooperation with EU institutions, in particular the European Commission, the Council of the EU, the European Parliament and EU Agencies. The new office will also liaise with national Permanent Representations to the EU and the Committee of Permanent Representatives, in order to bring company and sectorial views into the decision-making process. GMV will also work locally together with industrial partners, industrial associations, and local government to seek the best way of contributing to the growth of the sectors the company operates in.

GMV is a key contributor of EU Space flagship programs such as Galileo, Copernicus, SST, Govsatcom, Horizon Europe, with a strong role in implementation of Security and Defence agendas, particularly in the European Defence Funds (EDFs). From its Brussels office, the company will bring local presence to strengthen communication and coordination with EU on ongoing programs and new initiatives such as the Secure Connectivity Constellation, Quantum Encrypted Communications and Space Traffic Management.

The office located in the heart of the European Quarter in Brussels will be also be a place for stakeholders to meet up and swap views on EU industrial policy and programs.

GMV donates 50,000 euros to the Food Bank

The COVID-19 pandemic means that many employee events now have to be held online, often including some of sort of charitable money-raising effort. Such was the case of GMV's traditional Christmas get-together, also organized online and ending up with a charitable toast.

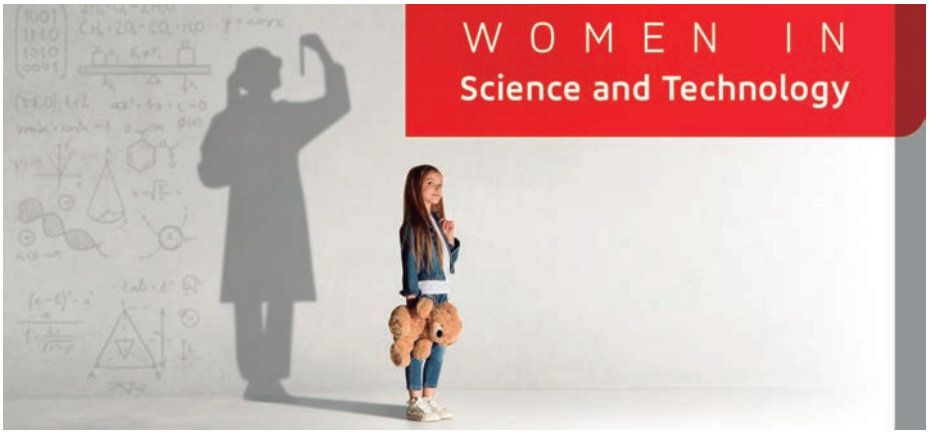
Mindful of the economic slump and food shortages caused by the pandemic, GMV's employees decided to turn their traditional Christmas gifts into a "charitable toast", raising a total of €35,860. This sum was topped up to €50,000 by the firm itself.

The Food Bank is one of the humanitarian organizations that are redoubling their efforts at the moment to deal with an avalanche of requests for food and basic necessities to fend off the healthcare, economic and social crisis unleashed by the COVID-19 pandemic.

This charitable gesture by GMV brings out the full importance today of the company's cultural and corporate values, large amongst which loom generosity, fellow feeling, cooperation and commitment. What more natural, therefore, than to support the Food Bank's humanitarian labors? This is only one outstanding example, moreover, of GMV's charitable endeavors over recent months, whether at corporate or individual level, to limit the damage of this pandemic.

The donation was handed over on 10 March by Ignacio Ramos Gorostiola, GMV's corporate manager of People Strategy & Infrastructures, on behalf of the whole firm and its employees.

Women in Science and Technology



On 11 February, under the aegis of the International Day of Women and Girls in Science, GMV held the webinar "Ciencia y Tecnología en Femenino" (*Women in Science and Technology*) to bring out the woman's role in science and technology and underline the importance of encouraging young women and girls to take up science-technology careers.

Webinar participants included Silvia Abarca, GMV space projects engineer; Ana Sastre, GMV defense software developer; Paloma Trigueros, head of healthcare digital services of GMV's Secure e-Solutions sector, and Cristina Muñoz, automotive project engineer for GMV's intelligent transportation systems.

The session brought out some of the main reasons behind this STEM gender imbalance, seeking to use this knowledge as a lever for change. The cultural aspect looms large here, especially in school curricula and the media.

Classroom gender equality translates into equal opportunities in the job market, leading in turn to a more balanced society as a whole. The aim is not feminization but rather to strike the right balance between men and women. For this to happen, women in science need to be given a higher profile with more media coverage. Young students have to be empowered through even-handed career guidance, while society's awareness has to be raised to debunk stereotypes, because talent, after all, is genderless.

GMV gets behind technology careers and STEM talent

Mindful of the urgent need to encourage and drive scientific research and STEM technology, GMV has been taking part for more than a decade in initiatives designed to steer students towards STEM careers

For over a decade now companies have been looking to universities and schools in search of future STEM professionals to meet the growing job demand. Not only did science, technology, engineering and mathematics (STEM) subjects fail to fill their classrooms, however, but takeup even continued to dwindle from year to year. This has a direct knock-on effect on the job market, making it extremely difficult for firms to attract the right talent and build up a sense of loyalty to the firm.

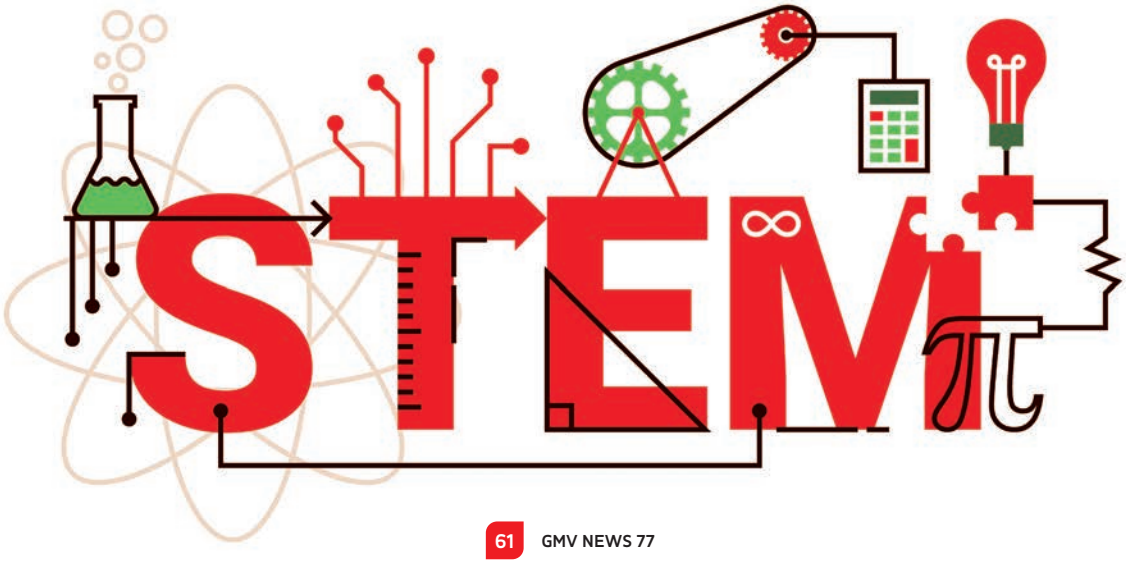
The situation is even worse on the female side, where technology career takeup has always been lower. In some STEM subjects women are still in the minority. More work is needed to break down those cultural barriers or stereotypes that might balk a proper awareness of science while giving a higher profile to example-setting role models who have made it in this field. According to the UNESCO study Cracking the Code only 35% of STEM students in higher education globally are women. Within research teams woman account for an even lower ratio of 28%.

Solving some of the stiffest challenges set by the UN's Sustainable Development Goals – ranging from improving health to tackling the climate change – will depend on harnessing all available talent. This means attracting both men and women to STEM careers. Greater diversity in research would broaden the talent pool and open up new viewpoints, develop capabilities and stimulate creativity.

Neither governments nor companies harbor any doubts nowadays about the need of driving scientific research and technology, while also encouraging youngsters to look at STEM careers. This involves promoting research-based training, bringing science's impact to wider notice, encouraging classroom ICT use and bringing in new educative resources.

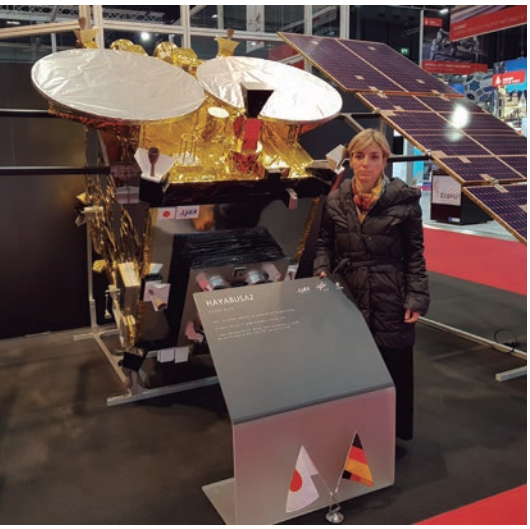
Never forgetting its academic roots, GMV collaborates in various events and organizes academic initiatives designed to spark off an interest in the technological world. Mindful too of the urgent and challenging need of promoting scientific research and STEM technology, GMV has been participating for over a decade in various initiatives designed to encourage students to take up STEM careers, especially initiatives geared towards female students.

GMV is supported in this ongoing task by some female mentors with scientific-technological skills who spend part of their time communicating their passion for STEM careers. In this article two of these women share their experience and give us their take on the importance of encouraging these careers.



Mariella Graziano

Executive Director of Strategy and Business Development/Flight Systems and Robotics. Aerospace



I've often been asked and even wondered myself why I chose to study engineering and the truth is I have no answer. I do know when the seed was sown. Even as a little girl I wanted to be a doctor. I went to Rome to enroll in the medicine school and came back as an engineering student, much to the chagrin of my family, who saw a broken link in the family's tradition of doctors.

The truth is I'm not a typical engineer, much less a space engineer. I've never liked science fiction; I've never seen a Star Wars film, or maybe I did catch one once. In my career everything has happened a bit by chance. I grew up in a tiny mountain hamlet where freedom and contact with nature were the going concerns.

I reckon I'm an engineer simply because I've always wanted to know how things worked. Although my grandmothers were humble, illiterate people, they were my first teachers and role models, teaching me with simple explanations of country people. Engineering has shown me that their teachings were true although the explanations are sometimes more complicated. There's not much difference in how a falcon or an aircraft flies. For me a moon landing is just as fascinating as watching a good pizza-dough rise. What makes the difference is knowing who you are and what makes you tick. This is what I try to get across when talking to budding talent.

I take part in many "STEAM" syllabi (I add in the A of Art because I believe creativity to be primordial for a good engineer, despite the fame of boring we're laden with), I've given chats to youngsters of all ages, from crèches up to universities. What I always do is talk about my own experience. I believe that nothing is so attractive and interesting to someone on the point of taking career decisions than real experience. I believe that our society exerts a heavy pressure on all youngsters but on girls in particular. Girls in a robotics competition have told me they signed up just to show that females could make a robot. I've always told them that this won't show anyone anything. This is all about doing what you like to the best of your ability and in the best company. This means you first need to know what you like and then it takes a lot of work and a dash of talent.

Aurora Izquierdo

Section Head. Intelligent Transportation Systems

When GMV encouraged me to take part in the "Stem Talent Girl" project, unknown to me at the time, I didn't hesitate. I loved the idea of serving as a role model to girls pondering a scientific-technological career. I myself never had someone to look up to like that, and although this lack didn't set me back, it will have undoubtedly nipped in the bud many brilliant scientific and engineering careers during several generations.

Although much remains to be done it is also true that each new generation of STEM girls is finding more role models of their own gender as well as men well aware of the importance of kindling scientific-technological careers in the 50% of the population that have historically tended to show less interest. Another crucial factor here is a cadre of teachers in our schools who know how to encourage both boys and girls from a very early age to give free rein to their curiosity and want to know why, the essential drivers of both science and engineering. In my case I was lucky enough to receive this stimulus in my student years.

I would therefore encourage anyone thinking about taking part in initiatives of this type to go right ahead. As well as being so necessary from a social point of view, this participation is also very rewarding on a personal level. And to the current students and future scientists and engineers I would say trust your instincts and go for it. You'll find far fewer obstacles in your path than your forerunners and help to make the path even easier for those who come after you.

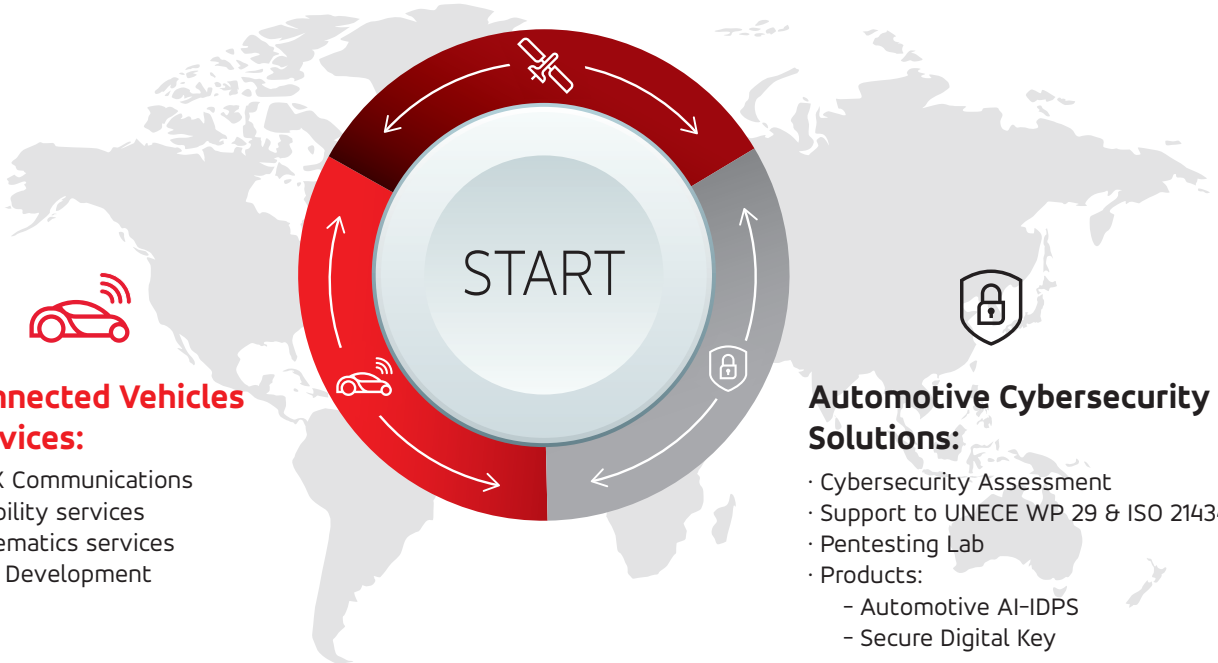
GMV Automotive Technology

GMV's automotive technology is based on 3 thrusts: GNSS-based autonomous vehicle positioning systems; automotive cybersecurity for developing specific products and services; the connected-vehicle area, bringing into the equation technology related to V2X communications, mobility services, telematic services and the development of secure and dependable software. These three thrusts are mutually complementary.

gmv_aut@gmv.com

GNSS Positioning Suite for Autonomous Driving:

· GNSS Precise and Safe Positioning Engine
· GNSS Correction Service



Connected Vehicles Services:

· V2X Communications
· Mobility services
· Telematics services
· SW Development

Automotive Cybersecurity Solutions:

· Cybersecurity Assessment
· Support to UNECE WP 29 & ISO 21434
· Pentesting Lab
· Products:
  - Automotive AI-IDPS
  - Secure Digital Key

gmv®
INNOVATING SOLUTIONS

GMV in the world

SPAIN
Headquarters
Isaac Newton 11 P.T.M. Tres Cantos - 28760 Madrid
Tel.: +34 91 807 21 00 Fax: +34 91 807 21 99

Santiago Grisolía, 4 P.T.M. Tres Cantos - 28760 Madrid
Tel.: 91 807 21 00 Fax: 91 807 21 99

Juan de Herrera nº17 P.T.Boecillo - 47151 Valladolid
Tel.: +34 983 54 65 54 Fax: +34 983 54 65 53

Albert Einstein, s/n 5ª Planta, Módulo 2 Edificio Insur Cartuja - 41092 Seville
Tel.: +34 95 408 80 60 Fax.: +34 95 408 12 33

Edificio Nova Gran Via, Avda. de la Granvia 16-20, 2ª planta
Hospitalet de Llobregat, 08902 Barcelona
Tel.: +34 932 721 848 Fax: +34 932 156 187

Mas Dorca 13, Nave 5 Pol. Ind. L'Ametlla Park L'Ametlla del Vallés - 08480 Barcelona
Tel.: +34 93 845 79 00 - +34 93 845 79 10 Fax: + 34 93 781 16 61

Edificio Sorolla Center, Nivel 1 Local 7, Av. Cortes Valencianas, 58 - 46015 Valencia
Tel.: +34 963 323 900 Fax: +34 963 323 901

Parque Empresarial Dinamiza. Avda. Ranillas, 1D - Edificio Dinamiza 1D, planta 3ª,
oficinas B y C - 50018 Zaragoza
Tel.: +34 976 50 68 08 Fax: +34 976 74 08 09

COLOMBIA
Capital Tower Bogotá, Calle 100 n.º 7-33, Torre 1, Planta 14- Bogotá
Ph.: +57 (1) 6467399 Fax: +57 (1) 6461101

FRANCE
17, rue Hermès - 31520 Ramonville St. Agne. Toulouse
Ph.: +33 (0) 534314261 Fax: +33 (0) 562067963

GERMANY
Münchener Straße 20 - 82234 Weßling
Ph.: +49 (0) 8153 28 1822 Fax: +49 (0) 8153 28 1885

Friedrichshafener Straße 7 - 82205 Gilching
Ph.: +49 (0) 8105 77670 160 Fax: +49 (0) 8153 28 1885

Europaplatz 2, 5. OG, D-64293 Darmstadt
Ph.: +49 (0) 6151 3972970 Fax: +49 (0) 6151 8609415

MALAYSIA
Level 8, Pavilion KL 168, Jalan Bukit Bintang, 55100 Kuala Lumpur
Ph.: (+603) 9205 8440 Fax: (+603) 9205 7788

POLAND
Ul. Hrubieszowska 2, 01-209 Warsaw
Ph.: +48 22 395 51 65 Fax: +48 22 395 51 67

PORTUGAL
Alameda dos Oceanos, 115, 1990-392 Lisbon
Ph.: +351 21 382 93 66 Fax: +351 21 386 64 93

ROMANIA
SkyTower, 246C Calea Floreasca, 32nd Floor, District 1, postal code 014476, Bucharest
Ph.: +40 318 242 800 Fax: +40 318 242 801

UNITED KINGDOM
GMV NSL
HQ Building, Bldg 77. 1st floor. Thomson Avenue, Harwell Science and
Innovation Campus, Didcot,Oxfordshire OX11 0QG
Ph: +44 (0) 1865954477 Fax: +44 (0) 1865954473

GMV NSL
Sir Colin Campbell Building. Innovation Park. Triumph Road
Nottingham NG7 2TU
Ph: +44 (0) 1157486800 Fax: +44 (0) 1159682961

USA
2400 Research Blvd, Ste 390 Rockville, MD 20850
Ph.: +1 (240) 252-2320 Fax: +1 (240) 252-2321

523 W 6th St Suite 444 Los Angeles, 90014
Ph.: +1 (310) 728-6997 Fax: +1 (310) 734-6831