gmv® INNOVATING SOLUTIONS NEWS

Nº65

AUGUST 2017

www.gmv.com

CYBERSECURITY
EVOLUTION, TRENDS AND NEW THREATS

INTERVIEW

ALBERTO
HERNÁNDEZ
CEO of Spanish National Cybersecurity Institute (INCIBE)

TALENT **Antonio Lozano Lima.** *"GMV's internships are full of opportunities, not only for the firm but also the students involved"*

rbr EVENTS

ATM & Cyber Security 2017

(formerly 'ATM Security')

#ATMsec

London 10th-11th October 2017

SEE US AT

ATM & Cyber Security 2017
LONDON (UK), 10-11 October 2017

ATM & Cyber Security 2017 is the world's leading conference focused on physical and logical ATM security. The event attracts over 340 delegates, representing more than 140 organizations from over 40 countries worldwide.

GMV, together with Trend Micro's Forward-looking Threat Research Department, will be given a paper under the title "The specific nature of ATM malware", explaining how ATM malware differs substantially from classic PC-oriented malware and how protection must adapt accordingly. This previously unpublished information will be given by David Sancho, Trend Micro's Anti-Malware Researcher, and Juan Jesús León, Director of Products and new Developments at GMV Secure e-Solutions.

More information:
https://www.rbrlondon.com/events/atmsec

gmv® INNOVATING SOLUTIONS

LETTER FROM THE PRESIDENT

Internet is a universal resource used daily by billions of people. Internet users, defined as anyone with access to a connection point and the basic knowledge necessary for using it, now account for 50% of the world's population. We use internet for keeping in touch with colleagues, friends and relatives, for watching films and videos, for moving our money about, for buying all kinds of articles, for reading books, for finding out the bus timetable or hailing a taxi, for obtaining information. Google runs 2.5 million searches per minute, tantamount to an average of one daily search by each internet user.

In addition to people, there is now an increasing amount of internet-connected devices. Only a decade ago internet was made up basically by computers. Then came smartphones and by now devices of all types are being connected up, including industrial sensors, household appliances and handhelds. This is the Internet of Things, or, more accurately perhaps, the Internet of Everything.

Internet and connected devices are revolutionizing our lives. Transactions that would otherwise be awkward, time-consuming or even impossible can now be done with a single click. The tradeoff is that we are handing over huge swathes of personal information and data that belongs to us. To post a message or a photo on social media may or not be wise depending on the circumstances, but it is an active decision. The same cannot be said of information sent by our smartphone, television set or the latest gadget we've got; all too often we're not even aware of the content or the addressee of this information. Big Data and Artificial Intelligence technologies will make it much easier to mine and exploit all this information. We must be aware of this and regain control of our data by means of Cybersecurity.

Mónica Martínez

Nº 65
AUGUST

CONTENTS

3 **LETTER FROM THE PRESIDENT**
MÓNICA MARTÍNEZ WALTER

6 **ARTICLE**
Cybersecurity. Evolution, trends and new threats

13 **INTERVIEW**
ALBERTO HERNÁNDEZ
CEO of Spanish National Cybersecurity Institute (INCIBE)

Published
GMV

Editorship-Coordination
Marta Jimeno, Marta del Pozo

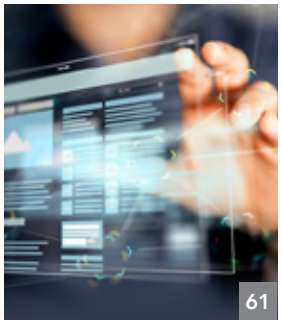
Area Heads
Antonio Hernández, Miguel Ángel Molina, José Prieto, Isabel Tovar

Writing
Neusa de Almeida, Amaya Atencia, Julián Barrios, Mariano Benito, Maole Cerezo, Iker Estébanez, Pedro Fernandes, Raquel Fernández, Teresa Ferreira, Fernando Gandía, Ángeles García, Celestino Gómez Javier Gómez, Bruno Gonçalves, David González, Sara Gutiérrez, Raúl Herbosa, Antonio Hernández, Pedro Lopes Vieira, Fátima López, Antonio Lozano, Belén Martín, Kamil Martin, David Merino, Daniel Montero, Héctor Naranjo, José Neves, Begoña Ochoa, Tatiana Pagola, Andrea Pellacani, Eric Polvorosa, Marta del Pozo, José Prieto, Pablo Rivas, Miguel Romay, Javier Sanz, Ian Sephton, Daniel Silveira, Juan Tejo, Javier Zubieta.

Art, design and layout
Francisco Huertas, Paloma Casero

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

6


61


34


53


48


45


20


13

18 **AERONAUTICS**
GMV contributes to the first transmission of an SBAS signal over Australia and New Zealand

20 **SPACE**
GMV, member of the consortium to supply Copernicus services in support to EU external action

34 **ROBOTICS**
GMV puts the LUCID rover through its paces

38 **DEFENSE & SECURITY**
GMV strengthens its position in the international defense and security market

44 **CYBERSECURITY**
Towards intelligence in Cybersecurity

48 **HEALTHCARE**
GMV innovation in European healthcare research projects

53 **ITS**
First takeup of the optimum planning system, ***gmv planner***

58 **AUTOMOTIVE**
First results of the ENABLE-S3 automation and self-drive project

61 **ICT**
The Inter-American development Bank (IDB) plumps for Knowledge management

66 **TALENT**
ANTONIO LOZANO LIMA. "GMV's internships are full of opportunities, not only for the firm but also the students involved"

On 13 May last, for the first time ever, a TV news broadcast opened with a cyberattack, namely the WannaCry attack, taking precedence over the usual headline-grabbing current affairs, sporting news or human-interest stories. This came as no surprise to GMV. In fact, such was its proven preparedness that it was even consulted during the news item as one of the experts, coming up with answers to such basic questions as "What happened?", "Why did it happen?", "How can the problem be dealt with and prevented from recurring in the future?"

Today's all-consuming digital transformation, which is certainly no passing fad or market trend, exposes the organizations concerned to attacks of this type. GMV was born as a digital firm, so it is well aware not only of the concomitant advantages of this digital transformation but also its inherent Cybersecurity problems, of which WannaCry is only one example. For this very reason GMV has been busily working away on its own and it clients' security since last century. It has by now built up the capability, resources and expertise to provide and ensure the desired levels of protection for each particular case. This protection is necessary not only because of the organizations' production or service-provision processes but also the soaring amount of information handled and generated during their activity nowadays.

This is no easy task. GMV itself might be hit by any scattergun attack. More particularly, as a groundbreaking company in a hi-tech market, it knows that its intellectual property, working methodologies or corporate software might all be specifically targeted by the hackers. These hackers are nowadays meticulously organized; they are working with the most efficient resources and are highly driven. They might be lurking in any country of the world, behind any connected equipment. This makes it extremely difficult to detect them beforehand and forestall their wrongdoing. It is an even greater hindrance to response actions.

Even so, GMV pulls it off. It does so on the strength of the nonstop dedication of its highly specialized Cybersecurity personnel, whose cutting-edge skills are constantly being updated. The company continually takes part in the forums and networks that discuss and analyze the very latest hacking technologies and vectors. It is further backed up by the whole company's undying pledge and determination never to be the weak link that might trigger a Cybersecurity attack. Innovation, creativeness and continual top-up Cybersecurity learning are other crucial ingredients in this mix. And all this is coordinated by means of methodologies, certifications and inhouse management systems, guaranteeing that every time any incident occurs GMV will be forewarned, prepared, bang up-to-date and on the case instantly.

GMV is therefore a guarantor of Cybersecurity. We are ready and waiting for anything the hackers might throw at us or any of our clients.

Mariano J. Benito
CISO
GMV SECURE e-SOLUTIONS

CYBERSECURITY
Evolution,trends and new threats

IN THE CURRENT SCENARIO WE NEED TO ASSUME WE ARE GOING TO BE ATTACKED. IT WOULD THEREFORE SEEM TO BE REASONABLE TO INCREASE OUR DAMAGE-LIMITATION EFFORTS. IT IS TRUE THAT THE MORE SOPHISTICATED IS THE ATTACK, THE HARDER IT WILL BE TO DETECT, AND THE LONGER WE TAKE TO DETECT IT, THE GREATER WILL BE OUR EXPOSURE TO THE RISK

CYBERSECURITY BECOMES A BUZZWORD

After the WannaCry attack of May 2017 "cyberattack", "ransomware" and "patch" all became household words, if only for a few days.

This situation, which has its upside and its downside, sometime comes in for heavy flak from the professionals. At least it raises the level of public awareness, something that has been called for now for a good few years. But we should not tip over into sensationalism. We need simply to lever this situation in order to raise the profile of Cybersecurity to its proper level, so that it can help to protect organizations, countries and individuals from cyberattacks.

Spreading the word is still an essential task. It is not a question merely of being excellent in your field but also demonstrating this and bringing it to the widest possible notice. GMV comes into its own here, playing an outstanding awareness-raising role in social media, academia and the media, both specialized and general, where we now consider ourselves to be opinion makers.

SOPHISTICATED ATTACKS CALLING FOR SOPHISTICATED RESPONSES

The threats we face today are well known, as well as the motives driving the perpetrators. Neither is the sophistication with which today's cyberattacks are arranged and unleashed anything new. What does need to change and improve is the response from the "good guys". In this case the best form of defense is not to attack but rather limit the damage and get back to normal as soon as possible, in one word: resilience.

In the current scenario we need to assume we are going to be attacked, whether in a sophisticated or slapdash manner. It would therefore seem to be reasonable to increase our damage-limitation efforts. It is true that the more sophisticated is the attack, the harder it will be to detect, and the longer we take to detect it, the greater will be our exposure to the risk. This risk can be mitigated using Cybersecurity intelligence, and this is something that we at GMV know how to do.

Intelligence depends on the analysis of a vast amount of information. For this purpose we use predictive-analysis technology, honed by us to suit the particular context in which it is to be used. In the fight against bank fraud, for example, we boast a wealth of experience in defining and refining "abnormal" behavior analysis algorithms to detect fraud attempts using Dridex type malware. Another example is the fight against ATM fraud, where we have been employing our ***checker ATM Security*** technology for over a decade now, building up to a position of world leadership.

VULNERABILITY MANAGEMENT, A GIANT STRIDE

Paradoxically, the level of sophistication of the attacks themselves often stands out in stark contrast to the sheer simplicity of certain constantly repeated methods. Almost all cyberattacks involve exploiting some sort of loophole at some moment, in other words taking advantage of an unsolved vulnerability. It is galling to find that many successful cyberattacks exploit vulnerabilities that have been known about for years and which are easily solvable by using a minimum kit of resources.

In speaking of risk we are referring to a combination of two factors: the probability of the threat actually occurring and the impact it is likely to have. Vulnerability management works mainly on the probability side of the equation, cutting it down significantly and thereby reducing the risk. If we now factor in the dependence of the vast majority of cyberattacks on an unsolved vulnerability, it stands to reason that a professional and well-articulated management of vulnerabilities could represent a giant stride forward in our race against the attackers.

A professional and well-articulated management of vulnerabilities could represent a giant stride forward in our race against the attackers

Vulnerability management is a well-known practice in any Cybersecurity department. It has been underway for many years now and is continually being honed and refined. A common-sense procedure has now been standardized, starting with the discovery, carrying on with the vetting and refinement, followed in turn by determination of the best corrective actions and ending with a feedback of information for those affected, all carried out in a cyclical manner to aid ongoing monitoring.

At GMV we have optimized this management process with ***gestvul***, an inhouse vulnerability-management service designed to fend off vulnerabilities in two especially complex contexts. Firstly, in scenarios where the number of assets is very high and any "stock" management procedure might fail disastrously due to a scalability problem. The second scenario is where the number of interested or affected parties is also very high, all of whom, critically, need to be informed in due form and time.

ME? … WHO'S GOING TO BOTHER TO ATTACK ME?

Sadly, it is all too often assumed that we are never going to fall victim to a cyberattack. Phrases like "Me? … Who's going to bother to attack me?" are all too often heard, especially in the industrial sector, where awareness of cyber risks is wanting and the cyberprotection measures taken by these companies are not as mature as might be desired, particularly in industrial networks and installations.

All the practical Cybersecurity experience built up in recent years, duly tweaked, could be applied to industrial environments. We could even lever the current drive towards Industry 4.0 initiatives or the Digital Transformation to phase in Cybersecurity from the very start of the whole process rather than tagging it on afterwards, when it would be too late. It should act as a facilitator and, as already pointed out above, three aspects are particularly crucial here: prevention, or maximum readiness for any threats; contention, to be able to minimize the impact of any attack; and recovery, to bring things back to normal as soon as possible after any contingency.

GMV has now built up a vast Cybersecurity expertise for industrial environments, especially in the energy and aerospace sectors. We take in the whole gamut of security levels and the security lifecycle models as defined in ISA/IEC 62443, analyzing the current situation by means of cyber-assessments, implementing protection measures in IT and OT networks, operating and monitoring the

defined controls. All this, moreover, is effected by means of a management system and governance framework taking in the whole activity of industrial Cybersecurity.

WORKFORCE SHORTAGE

A constant feature has emerged in 2017: a worldwide shortage of Cybersecurity experts. Pundits are now predicting a workforce shortage of between 1.5 and 2 million by 2019.

The difficulty of coming up with highly skilled in-company personnel means that companies are extremely demanding when outsourcing their Cybersecurity service to an expert like GMV. In particular they call for specialization (one-size-fits-all services will not do) and due adaptation to the organization concerned in each case (standardized and rigid services will not do either; they must be totally flexible and adaptable to each client's business culture and day-to-day reality). Or what comes to the same thing: aptitude + attitude.

In truth these requirements have always been there. The new feature now is the current sophistication, reaching a level nowadays of completely bespoke services. As a result we build up such a deep and specific knowledge in each case that there can be a positive knock-on effect for other clients, especially those who belong to the same sector.

ALL-ROUND COMPLIANCE AND LAW-ABIDANCE

Cybersecurity nowadays is closely bound up with law abidance and standard compliance. Companies set up their own internal rules and standards that are binding on all employees throughout the whole organization. To this must be added external laws and regulations.
In Spain this boils down to the Spanish Data Protection Law (*Ley Orgánica de Protección de Datos*: LOPD) and the Critical Infrastructure Protection Law (*Ley de Protección de Infraestructuras Críticas*: LPIC); some sectors additionally apply specific regulations, such as the requirements of the European Central Bank (ECB) to be met by banks and financial institutions or the National Security Scheme (*Esquema Nacional de Seguridad*: ENS) to be complied with by Spain's public authorities.

A watershed Cybersecurity moment is looming up in 2018 with enforcement of the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) directive, which will pool, develop and override some of the abovementioned laws. The GDPR is hogging all the headlines due to its binding impact on practically any type of organization, and its compliance looks likely to be complex.

Legislation "overkill" is a fairly familiar phenomenon for firms like GMV. This new set of laws and regulations is by no means the first (neither will it be the last) we have to tackle, not only on our own account but also for helping our clients. Within the set of by-now consolidated laws we have repeatedly analyzed client risks, brought the security scheme into line with them, implemented the required Cybersecurity measures and monitored compliance afterwards.

What does the future hold?

Certain events are occurring today that enable us to venture a forecast of the near future of Cybersecurity. There are several key facts and figures to work from. Take the following examples: Spain's National Cybersecurity Institute (*Instituto Nacional de Ciberseguridad*: INCIBE) dealt with 115,000 incidents in 2016 (130% more than in 2015); according to the Cisco 2017 Annual Cybersecurity Report, 90% of organizations that reported a security breach then go on to improve their threat defense technology; the IDC in its 2017 Global Security Product & Service Predictions, forecasts that by 2019 more than 75% of IoT device manufacturers will improve their security and privacy capabilities and that by 2018 70% of enterprise Cybersecurity environments will use cognitive/AI technologies to assist humans in dealing with the vastly increasing scale and complexity of cyber threats.

At contextual level the IoT scenario poses a stiff protection challenge. This

THE EXPERT OPINION

ARE WE PREPARED FOR CYBERATTACKS OR IS THERE STILL UNFINISHED BUSINESS? THESE AND OTHER QUESTIONS WE HAVE PUT TO THE EXPERTS

MARIA JOSÉ
GARCIA
Information Systems Manager - Universidad Autónoma de Madrid (UAM)

What role does Cybersecurity play within your organizations?

The Universidad Autónoma de Madrid, as a public authority, is bound by Royal Decree 3/2010 regulating Spain's National Security Scheme (*Esquema Nacional de Seguridad*). Solely on a law-abidance level, therefore, we have to keep Cybersecurity constantly in mind. On top of that, however, Cybersecurity is critically important to underpin and ensure the university's daily activity, bringing together as it does an average of 50,000 users a day with very diverse online behavioral patterns and profiles. To this must be added a further security complication and uncertainty: the visiting students and researchers from other universities who connect up their own equipment to our network.

We are well aware of the importance for user protection of keeping software bang up to date, distributing as soon as possible the latest updates. This helped to safeguard the university from the famous WannaCry attack, since Microsoft's virus-protection update had already been installed in the computers of teaching, administration and service staff.

What is the reason for the increase in cyberthreats and how are you dealing with them?

During the last year we have detected a huge increase in malicious traffic while stepping up our network scans, particularly those related to Mirai and similar IoT-targeting BotNets. Suffice it to say that 80-85% of internet connection requests are turned down by our protection measures.

We are also noting a very worrying increase in DDoS type attacks, albeit with only a very slight effect on us as yet. But we need to bear in mind here that the hackers' wherewithal is becoming cheaper by the day, making their attacks easier and more affordable.

What general trends do you foresee?

The increasing rate of e-government digital services makes it essential to harden up the security of services implementing specific security rules.

Along these lines, in 2015 the university approved the Information Security Policy, while the governing board is continually approving and phasing in new general security rules and procedures.

We have also recently conducted the first Business Impact Analysis or BIA on critical services. At the moment we are in the phase of estimating the necessary resources for ensuring the target recovery time. We will also continue to develop ENS-related rules and procedures.

Lastly, another point we need to reinforce is our users' awareness of information security matters. The recent

problem needs to be tackled from a holistic viewpoint, starting with the security of the IoT devices themselves (preferably built-in from the start), followed by connectivity (with special concern for the Cloud) and ending up with the final systems that record all generated data or serve as management platforms (data is considered to be the most valuable assets of all).

At technology level we can harness all the breakthroughs now being made in artificial intelligence and learning and apply them to new data-analysis algorithms from a Cybersecurity perspective. This will allow us to flag up hard-to-detect suspicious behavior, head off future problems and manage resources more efficiently.

At threat level we will continue to see many ransomware-like kidnaps, whether sophisticated or not. As things stand the kidnappers come out winning because the initial outlay to perpetrate the attack is minimal, the potential impact is huge and the chances of being caught are low. As has happened before (e.g. with the spam of the noughties), the fight against ransomware is likely to end up exterminating it, unless it mutates into another type of attack or simply falls out of fashion.

headline-grabbing incidents have helped us to convince the governing team of the importance of establishing Cybersecurity rules. But it is also at least equally important for our users to understand the measures taken and collaborate willingly in their enforcement.

RAMÓN ORTIZ
Security Manger - Mediaset

What role does Cybersecurity play within your organization?
The traditional reactive role of Cybersecurity is now giving way to a more proactive, essential and across-the-board approach in digital-transformation, engineering and app-development projects, in system operations and differentiated business initiatives.

Technology is a hallmark of Mediaset's business and mindset. As such, the security measures to be adopted are essential as a guarantee of integrity, availability and confidentiality (+swiftness) of the company's service and information assets and as an efficient way of winning and keeping up confidence and trust in the services rendered and in the image of grupo Mediaset for the audience of our TV channels, the users of our websites and our clients and advertisers.

What is the reason for the increase in cyberthreats and how are you dealing with them?
It's obvious that the number, variety and gravity of attacks are increasing year by year, as well as the expertise of the hackers. There is as yet no convincing consensus about the reason for this increase and honing of attacks and incidents.

Some pundits are arguing convincingly that cybercrime is now picking up on certain capacities and skills that were hitherto within the scope only of government agencies. If this is true, then companies and organizations, regardless of their size and wherewithal, are in for a torrid time unless they make nonstop efforts to update and revise their prevention and control measures.

What general trends do you foresee?
In view of the abovementioned scenario, Mediaset's forecasts pretty much chime in with general expectations.

Constant malware alert. Work constantly on the advanced configuration of antimalware tools, explore the use of behavior analysis techniques.

Improvements in mobile device management. The goal in sight is maximum convergence of the same security measures in mobile devices as in traditional client equipment. In other words, making MDM not only a management- but also a protection-tool. Avoid transference of information between personal and professional apps contained on the same handheld.

Build Awareness. Working with the right training plans, raise awareness of the importance of Cybersecurity among Mediaset's staff and executives and of their active security-boosting role in terms of responsible behavior. Mediaset's commitment to inform society of its security and privacy rights.

Security in cloud environments. Adopt access, monitoring and architecture-design controls alongside the design of on-premise corporate environments, making security equivalent in both spheres. Adoption of practices and tools for controlling the use and consumption of deployed resources as an additional control to cloud-hosted platforms.

Legislation. Existing legislation is soon to be enhanced and extended by new requirements and rules. Each organization, depending on its sector, will be affected to a greater or lesser extent by these new security rules.

RAÚL
HERBOSA
Director of Information Systems, GMV

What role does Cybersecurity play within your organization?

In such a fiercely competitive world we all tend to focus on our daily tasks and leave Cybersecurity up to the IT department: "It's their job". On other occasions the problem is wrongly couched in terms of liability; "Am I covered from any attack? Could I be held liable for the consequences?"

These approaches are clearly misguided from all points of view. This is everyone's problem, and all of us, within our own possibilities, are duty bound to make our own contribution towards a proper level of protection, by setting the right example in our own daily tasks and helping to raise awareness of good practices as a prevention measure. Sadly, awareness is all too often raised only by a specific incident or a general event that hits the headlines and trips all the alarms.

In GMV we have an extra level of awareness since Cybersecurity is an important part of our business. This means we cannot afford the luxury of lamenting risk-management lapses afterwards. We need to have all our information systems prepared for any possible attack, as far as this is humanly possible.

What is the reason for the increase in cyberthreats and how are you dealing with them?

In such a globalized world as today's, with such a crisscross of vested interests, it is by no means farfetched to imagine future cyberattack "wars" that shake the very foundations of countries remotely without any bloodshed. What we are witnessing now is a spiraling upward trend year after year in the number of attacks and the number of existing cyberthreats.

Our department tackles this issue shrewdly, working from the maxim that "there is no such thing as perfect security". We therefore don't let down our guard at any moment. The fact that we have never yet been affected by any of the most widespread attacks by no means lulls us into a false sense of security.

What general trends do you foresee?

The trend of recent years tells us that cyberthreats and attacks are bound to increase in the future. There is no sense in being alarmist, but equally senseless would be to sit with our arms crossed hoping against hope to be spared the latest threat to economic, political, religious interests, etc.

The advent and boom of new technologies like IoT, mobile devices, Wi-Fi networks or Cloud solutions make it more necessary than ever to define our own Cyberdefense procedure that enables us to keep up a reasonable level of security and alert, duly adapted to each business so that all the productive processes associated with our firms can carry on nonstop.

GMV systems department team

ALBERTO HERNÁNDEZ

CEO OF SPANISH NATIONAL CYBERSECURITY INSTITUTE (INCIBE)

THE NATIONAL CYBERSECURITY INSTITUTE (*INSTITUTO NACIONAL DE CIBERSEGURIDAD*: INCIBE) IS A PUBLIC CORPORATION DEPENDENT ON THE STATE SECRETARIAT FOR THE INFORMATION SOCIETY AND THE DIGITAL AGENDA UNDER THE MINISTRY OF ENERGY, TOURISM AND THE DIGITAL AGENDA. IT'S MAIN REMIT IS TO PROVIDE SPAIN'S PRIVATE SECTOR AND CITIZENS WITH PUBLIC CYBERSECURITY SERVICES, FOCUSING ESPECIALLY ON PRIVATE OPERATORS OF CRITICAL INFRASTRUCTURE UNDER A COLLABORATION AGREEMENT WITH THE MINISTRY OF THE INTERIOR THROUGH ITS NATIONAL CRITICAL INFRASTRUCTURE PROTECTION CENTER (*CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS*: CNPIC). AS A RESULT OF THIS COLLABORATION AGREEMENT A COMPUTER EMERGENCY RESPONSE TEAM (CERT) WAS SET UP. INCIBE'S CEO, ALBERTO HERNÁNDEZ, TALKS US THROUGH THE WORK IT CARRIES OUT AND THE MAIN CHALLENGES LOOMING UP AS "GUARDIANS" OF CYBERSECURITY.

WHAT ARE THE MAIN AREAS YOUR INSTITUTE'S ACTIVITY FOCUSES ON?

Our overriding remit is to work as a public service, based on prevention and raising public and corporate awareness about the secure use of technologies, humanizing Cybersecurity.

INCIBE's other main activity is to identify the capacities needed for proactive detection of cyberattacks affecting Spain's citizens and private sector, in order to locate them, analyze them and bring them to the knowledge of the affected parties.

HOW DO YOU TACKLE THIS?

INCIBE's approach is very hands off. We don't actually monitor the activity of citizens or companies. Working within the framework of national and international collaboration agreements, we set up information-exchanging arrangements, either through international Cybersecurity companies or by acquiring information sources. This allows us every year to analyze over 10 million incident-related information events in Spain and detect about 100,000 infected networks daily in Spain. INCIBE is an international anti-bot service benchmark, a groundbreaking service at world level. Thanks to the collaboration of Internet service providers (ISPs) such as telecommunications operators we can identify proactively the IPs of users infected by some type of malware. We detect infections, analyze what's going on, trace the problem to its origin, ascertain what the incident consists of and pass this information on. This stresses the crucial importance of everyone working together towards the most bullet-proof Cybersecurity. Collaboration between the public and private sectors is vital for the proper protection of our citizens and firms.

THIS IS A DELICATE POINT, SINCE WE ARE TALKING ABOUT SHARING INFORMATION. WHICH MEASURES DO YOU SEE AS LIKELY TO BE MOST EFFECTIVE IN OBLIGING THE PRIVATE SECTOR TO SHARE ITS INFORMATION WITH THE PUBLIC IN THE COLLECTIVE STRUGGLE AGAINST CYBERCRIME?

The European Union's directive concerning measures for a high common level of security of network and information systems, as implemented in Spain, makes it obligatory for companies running essential services to report any security incidents. It is very important here to work on early warning; rather than compulsoriness itself we need to focus on explaining and understanding the benefits of prevention. The sharp rise in incidents dealt with in 2016 as compared to 2015 (from 50,000 to 115,000) is due to three main factors: the greater detection capacity as a result of a bigger outlay, better communication between companies and citizens and, lastly, the global increase in incidents. We are now noting a benefits-driven increase in the quantity and type of information we are being furnished with from the private sector.

WHAT ABOUT PRIVATE ORGANIZATIONS THAT ARE NOT OPERATORS OF CRITICAL INFRASTRUCTURE? FOR THE LATTER THE SITUATION IS TIGHTLY REGULATED, BUT HOW SHOULD THE FORMER CONTACT AND LIAISE WITH INCIBE?

From a preventive point of view, logging onto the website and getting involved in our projects. For example, we offer an awareness-raising kit; any firm can now download an awareness-raising plan and all the necessary wherewithal for implementing it. We offer a set of very simple tools to find out the organization's risks, ranging from gaming elements with interactive itineraries for employees to an online game to check out their level of knowledge.

> COLLABORATION BETWEEN THE PUBLIC AND PRIVATE SECTORS IS VITAL FOR THE PROPER PROTECTION OF OUR CITIZENS AND FIRMS

For anyone who has suffered a cyber incident there are two options. The first is to report the incident to the state security forces; the second is to do so through the security and industry CERT we run from INCIBE. We can then help out in the analysis of the problem and give them an answer. As for the ransomware attacks that are nowadays hitting the headlines, largely flying under the radar beforehand, we run a free public decryption service with a success rate of over 80%.

Another good idea is to get involved in the activities run from INCIBE in

collaboration with Cybersecurity firms. These include awareness-raising activities and other free, country-wide initiatives designed to give entrepreneurs a much better idea of Cybersecurity.

YOU'VE MENTIONED COLLABORATION WITH THE NATIONAL CYBERSECURITY INDUSTRY. HOW IS THIS SET UP AND ORGANIZED?

What we call a technical Cybersecurity pole has been set up. This is a space where we seek synergies between the industry's concerns and the action of public organizations. We at INCIBE support national industry's internationalization and competitiveness. As a body dependent on the Ministry of Energy, Tourism and the Digital Agenda we are very interested in the industrial development of Spain and the generation of jobs. We therefore work jointly with the Cybersecurity industry to pinpoint activities likely to improve the competitiveness of Spain's industry, boosting its level of internationalization. We have set up a Digital Trustworthiness Plan (deriving from the Digital Agenda for Spain) to determine industry's Cybersecurity demand in upcoming years so that the Cybersecurity sector can develop products and services to suit while also working with national Cybersecurity-oriented R&D centers. Within this Plan INCIBE has led the setting up of a Network of R&D Excellence Centers with the aim of pooling current efforts and running the activity in a more coordinated way under a future master plan in line with the European strategy and the real needs of industry and end users. Another activity is the annual holding of National Cybersecurity R&D Days (*Jornadas Nacionales de I+D+I en Ciberseguridad*: JNIC), which act as a meeting point between the various Cybersecurity research stakeholders (universities, technological and research centers, companies and government authorities) for swapping notes with the common aim of driving national-level Cybersecurity research. Another form of collaboration is promoting startups.

AND WHICH OTHER INSTITUTIONS, LIKE THE CDTI, SUPPORT INITIATIVES OF THIS TYPE? HAVE YOU SIGNED ANY ENTREPRENEURSHIP-SUPPORTING AGREEMENT?

Indeed, other public organizations working jointly with us are the Industrial Technology Development Center (Centro para el Desarrollo Tecnológico Industrial: CDTI), the Foreign Trade Institute (Instituto de Comercio Exterior: ICEX) for internationalization purposes and ENISA Spain, whereby we support entrepreneurship, internationalization and the generation of startups. The industry is also present in the various phases of the business acceleration process, either in advisory committees, science committees or the actual project-selection tribunal, via such initiatives as "Cyber-emprende" or "Cybersecurity Ventures", an international business accelerator that we have set up together with the Regional Authority (Junta) of Castilla y León and the City Council (*Ayuntamiento*) of León. This line of work would be pointless without the collaboration of the Cybersecurity industry itself. Recently, to tackle the WannaCry and Petya ransomware cyberattacks, INCIBE worked jointly with the National Cryptology Center (*Centro Criptológico Nacional*) the Joint Cyberdefense Command (*Mando Conjunto de Ciberdefensa*) the Guardia Civil, the police, specialist research units, but also with representatives from the Cybersecurity industry. During this period real-time information-exchanging arrangements were set up. Thanks to all this collaboration the impact of these cyberattacks was limited in Spain.

WHAT WOULD BE YOUR SNAPSHOT OF THE NATIONAL CYBERSECURITY INDUSTRY AT THIS MOMENT? HOW DOES ITS DEVELOPMENT MEASURE UP TO OTHER COUNTRIES AND TO THE ICT INDUSTRY IN GENERAL?

INCIBE- We have pinpointed about 130 to 140 companies we call "Pure Cybersecurity Players" i.e., companies that run a Cybersecurity business unit or have products/services in Spain.

They are all companies trading in Spain, including multinationals. We see them still as thin on the ground and patchy in size, with a predominance of small firms. In comparison with other countries this is a small, though fleet-footed and efficient industry and it holds its own on the international market.

WANNACRY WAS A WATERSHED MOMENT FOR SPAIN. FROM THAT MOMENT ON BOTH COMPANIES AND THE PUBLIC AT LARGE HAVE BECOME MUCH MORE AWARE OF THE IMPORTANCE OF CYBERSECURITY

HOW DO YOU SEE THE FUTURE DEVELOPMENT OF THE CYBERSECURITY SECTOR?

Our studies of Cybersecurity trends show that the major or consolidated companies will continue to grow, with a parallel opportunity for the generation of startups. The intrinsic fleet-footedness of small companies and entrepreneurs enables them to break into niches or markets overlooked by the major firms. We believe there are opportunities for both. In fact our study of last year's trends concludes that the Cybersecurity industry will be led by major firms with significant leeway for small and medium-sized firms on the strength of a crucial ICT factor: disruptive innovation. We have seen garage-born firms with a disruptive idea sprout into fully-fledged multinationals in no time. We believe this will be a differentiating factor for many years to come, favoring the appearance of small firms and allowing consolidated firms to carry out their projects and incorporate new products and services.

WOULD YOU SAY SPAIN'S STATE COMES UP WITH THE NECESSARY CYBERSECURITY RESOURCES?

The state's current general budgets have earmarked a sufficient amount for the current context. On an upbeat note INCIBE's budget has experienced a significant percentage increase, showing that the state is behind us. Should we be investing more? From a global point of view, money is now required for healthcare, for education… What we are looking at is an increase of the Cybersecurity budget in keeping with Spain's resources.

INCIBE HAS VERY FEW COUNTERPARTS IN OTHER COUNTRIES. DO YOU KNOW ANY PRECEDENTS OF SIMILAR INSTITUTIONS PLAYING A ROLE OF INSTITUTIONAL CYBERSECURITY SUPPORT, NOT ONLY PUBLIC BUT ALSO PRIVATE?

One factor that makes INCIBE stand out from the rest is its international projection, with a twofold objective: to set up information-exchanging collaboration arrangements and project an image of a strong international position for our industry. It is perhaps this second goal that sets INCIBE apart even more from other European initiatives, which are limited to mere agencies centering on the country's security. In Latin America, as international experts, we support the development of national Cybersecurity strategies of various countries, often taking INCIBE as their role model.

WHAT'S YOUR TAKE ON THE DIGITAL TRANSFORMATION BOUND UP WITH THE FOURTH INDUSTRIAL REVOLUTION? ARE THESE SECTORS READY IN CYBERSECURITY TERMS FOR THE CHALLENGE POSED BY THE INTERCONNECTION OF THEIR PRODUCTS AND SERVICES?

Digital transformation is turning out to be a very fast process, perhaps with scant regard for Cybersecurity. WannaCry was a watershed moment for Spain. From that moment on both companies and the public at large have become much more aware of the importance of Cybersecurity, looking at it as an investment.

WHAT DO YOU SEE AS THE GREATEST BARRIER TO ALL THESE DIGITALIZING INDUSTRIES TAKING ON CYBERSECURITY AS AN ESSENTIAL PART OF THEIR ACTIVITY?

There is obviously an economic barrier because of the necessary outlay, but this has to be weighed up against the benefits. I believe we are now in a better situation than before; entrepreneurs are beginning to understand that it is necessary for their business.

A KEY ELEMENT, PERHAPS STILL UNSOLVED, IN THE DIGITAL TRANSFORMATION IS THE AVAILABILITY OF DIGITAL TALENT. WHAT'S THE CYBERSECURITY SITUATION LIKE?

Studies point to a considerable shortfall of Cybersecurity talent in Europe. A 2014 study forecast that this shortfall will add up to nearly 700,000 unfulfilled jobs by 2017 and about one million by 2020. In Spain there are between 5000 and 6000 professionals working in the Cybersecurity area, so the demand is smaller, but there is still a significant gap that needs to be bridged. We organize an annual event called Cybercamp to give parents, children and budding talent a better idea of Cybersecurity. Last year's Cybercamp in Leon attracted a turnout of nearly 20,000; over 2200 vacancies were advertised and free training initiatives were held, but we received barely 900 résumés. This shows a very big gap and the need for a program to promote Cybersecurity skills and interest among 14-, 15-and 16-year-olds. We at INCIBE are setting up initiatives to attract budding talent to this sector and help them make contact with companies. There's still some way to go, but we believe we're on the right road. Last year, for example, in the European Cyber Security Challenges, the Spanish team, made up by 10 youngsters cherry-picked in Cybercamp, came out as champion of Europe. This shows there is talent in Spain and that the activities we are carrying out are now bearing fruit.

AND FOR WOMEN, DO YOU DRIVE ANY EQUALITY-FAVORING ACTIONS?

Working on gender diversity has been identified as one of the goals set by the Secretary of State for the Information Society and Digital Agenda, José María Lasalle, within the new digital agenda for Spain, ensuring that women are playing their rightful part in this endeavor. This year, in collaboration with the Organization of American States (OAS), we are putting on the "1st International Forum of Gender and Cybersecurity" to encourage a more inclusive digital world and analyze the current situation and gender problems both at national and international level in the Cybersecurity sector. The idea is to continue working on defining and developing strategies to ensure this gender diversity within the world of Cybersecurity.

GOING BACK TO THE RANSOMWARE SCENARIO. . . A LITTLE MORE THAN A YEAR THERE WERE ATTACKS ON THE HEALTHCARE SECTOR IN THE UK AND USA. WHY DO YOU THINK THIS PARTICULAR SECTOR WAS TARGETED? WOULD YOU SAY SOME SECTORS IN SPAIN ARE MORE ATTACKABLE THAN OTHERS?

An X-ray of incidents in Spain shows a higher rate in the technologically more advanced sectors, with an increase in technology-investing sectors that hardly recorded any incidents three years ago, making them more prone to cyberattacks. We are working flat-out on the Cybersecurity of industrial control systems, trying to bring in Cybersecurity from the design stage upwards and ensure secure internet access.

MicroSMEs, accounting for the majority of firms in Spain, are tapping into more and more technology. They usually, however, lack a proper security level, either from ignorance or complacency. We therefore have to stress the need of humanizing Cybersecurity and working together, not only at INCIBE, to get across the idea that a modest outlay can achieve high protection levels.

HOW DOES SPAIN RATE IN TERMS OF CYBERSECURITY R&D?

Countries of Spain's size would come out both above and below Spain in terms of R&D investment. Countries working with a bigger budget (USA, UK) leave us well behind, although Spain does stand out in some aspects: we are efficient and we boast good talent. We have to continue along this path, nurturing talent and encouraging our firms to develop their ideas and sell them abroad.

GMV HAS BEEN WORKING WITH INCIBE FOR 10 YEARS NOW. WHAT WOULD YOU HIGHLIGHT ABOUT THIS ONGOING COLLABORATION?

We believe you've carried out excellent work, vouched for by many years of collaboration in essential projects for our activity. Your international outlook sets an upbeat example of a firm capable of meeting needs at home while also making great inroads abroad.

Luis Fernando Álvarez-Gascón, General Manager of GMV Secure e- Solutions and Alberto Hernández, CEO of INCIBE

In the next phase of the project GMV will contribute to the start of transmission of a second generation SBAS signal. This signal will provide to the GNSS users of a double SBAS and PPP service, including the extension of the augmentation to both GPS and Galileo satellites

GMV contributes to the first transmission of a SBAS signal over Australia and New Zealand

Last June GMV contributed to the first transmission of a SBAS signal through a geostationary satellite over Australia and New Zealand. Satellite-based Augmentation Systems (SBAS) improve the accuracy of positioning and integrity of GPS satellites. These systems has already been rolled out in the United States (WAAS), Europe (EGNOS), India (GAGAN) and Japan (MSAS).

This first transmission is done as part of the strategy of the Australian and New Zealand governments for the development of positioning infrastructure in the Australasia region. The project will lasts two years and is coordinated by Geoscience Australia (GA) and the Cooperative Research Center for Space Information of Australia and New Zealand (CRCSI). GMV, Lockheed Martin and Inmarsat collaborate on the project by providing the infrastructure for the generation and transmission of SBAS messages.

The objective of the project is to show the potential benefits of satellite navigation technologies including integrity and high precision services. With this purpose, in the coming months, various experiments and tests will be carried out using the SBAS signal in various sectors such as agriculture, construction, mining or transportation, among others.

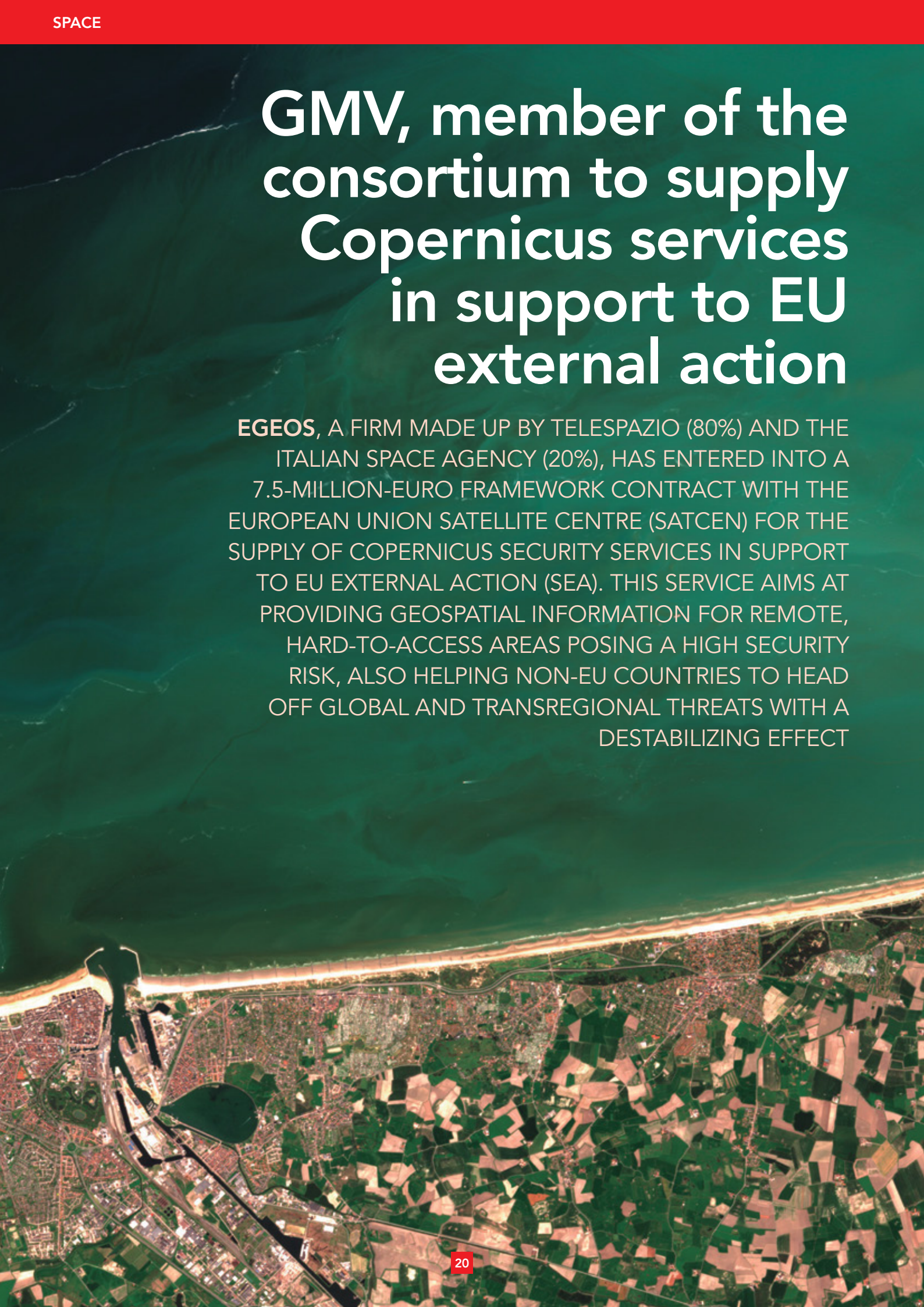
For the development of the infrastructure, Geoscience Australia (GA) has selected a GMV for the provision of process elements in charge of the generation of SBAS messages and user equipment, Lockheed Martin for the signal link with the geostationary satellite, and Inmarsat for the SBAS payload in the geostationary satellite.

Last May, two GMV engineers moved to the Lockheed Martin facility in Uralla, New South Wales (Australia) to participate in the installation and integration of the infrastructure. Early in June, Geoscience Australia together with the Australian aviation authorities authorized the start of the signal transmission.

In the next phase of the project GMV will contribute to the start of transmission of a second generation SBAS signal. This signal will provide to the GNSS users of a double SBAS and PPP service, including the extension of the augmentation to both GPS and Galileo satellites.

GMV, member of the consortium to supply Copernicus services in support to EU external action

EGEOS, A FIRM MADE UP BY TELESPAZIO (80%) AND THE ITALIAN SPACE AGENCY (20%), HAS ENTERED INTO A 7.5-MILLION-EURO FRAMEWORK CONTRACT WITH THE EUROPEAN UNION SATELLITE CENTRE (SATCEN) FOR THE SUPPLY OF COPERNICUS SECURITY SERVICES IN SUPPORT TO EU EXTERNAL ACTION (SEA). THIS SERVICE AIMS AT PROVIDING GEOSPATIAL INFORMATION FOR REMOTE, HARD-TO-ACCESS AREAS POSING A HIGH SECURITY RISK, ALSO HELPING NON-EU COUNTRIES TO HEAD OFF GLOBAL AND TRANSREGIONAL THREATS WITH A DESTABILIZING EFFECT



The contract entails analysis of a large number of round-the-clock satellite images. To provide the associated value-added products e-GEOS is leading a European consortium comprising GMV, GAF, Telespazio Ibérica, Airbus DS, IABG and SIRS. GMV, as a member of this powerful team of industrial operators, will be providing operational geospatial-production services in support to EU external action.

The geospatial support service consists of earth-observation image analysis services with a consolidated portfolio of products for various service-activation intensity levels. The contract will be operative round the clock on the basis of user-driven, SatCen-activated operation orders. SatCen will thus act as liaison between users and industry and will weigh up the quality of the final products.

GMV offers two production centers (Spain and Portugal) to carry out internal assessments of map quality as support to strategic and decision-making processes. GMV has the capability for generating any portfolio product of this Copernicus service and will support general project management by carrying out the quality management function. This function centers on offline assessment of product quality, alongside the SatCen validation exercise with the purpose of pinpointing constant faults caused by inadequate workflow. Ensuing comments will help to improve the map-production chain and product quality, reducing reprocessing needs due to low quality and hence improving delivery times. GMV will also be developing a production-order management interface, giving detailed information on the process and associated resource consumption.

The Copernicus program sets out to obtain an autonomous earth-observation system working from a satellite network, a network of ground measurement stations and airborne sensors and also the generation of information services. The overarching aim is to observe the planet from all possible viewpoints to gain a better understanding of the changes underway and how they will impinge on our daily lives.

For their part, Copernicus services will see the transformation of in situ satellite data into value-added information by processing and analyzing same, phasing them in with other sources and validating results.

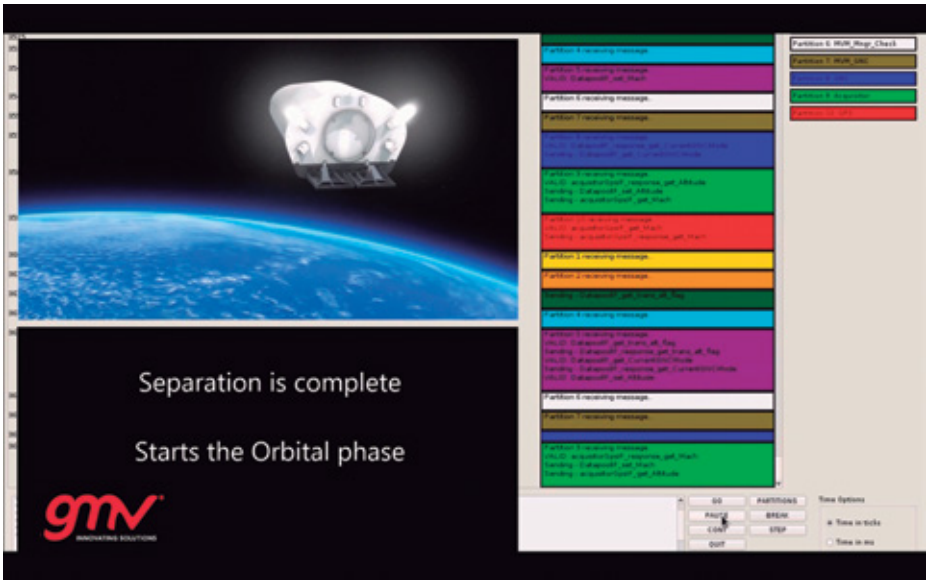
MORA-IMA combines major technological goals on Embedded Space Software

THE EUROPEAN SPACE AGENCY HAS ONCE MORE TURNED TO GMV´S EXPERIENCE IN BOTH OSRA (ONBOARD SOFTWARE REFERENCE ARCHITECTURE) AND IMA (INTEGRATED MODULAR AVIONICS). THE GMV- LED TEAM IN PORTUGAL WILL DEVELOP A "MULTICORE IMPLEMENTATION OF THE ONBOARD SOFTWARE REFERENCE ARCHITECTURE WITH IMA CAPABILITY" (MORA IMA)

OSRA is a single, agreed and common solution for the definition of the software architecture of onboard software systems, enabling a fast, model-based software development process.

IMA, also known as Time and Space Partitioning (TSP), is a paradigm that has been widely adopted in several industries, allowing the execution of highly critical software mixed with non-critical software. This mixed criticality is achieved through the isolation (partitioning) in time and space of the software applications that compose the avionics system. Furthermore, IMA/TSP is an elected possible solution to future multi-core computers, following a philosophy of associating processor cores to partitions.

MORA-IMA will combine for the first time ESA's three major technological goals concerning Embedded Space Software



The purpose of MORA-IMA is to demonstrate the feasibility and evaluate the performance of an end-to-end process, tools & building blocks from application level specification using the OSRA approach down to implementation of combined OSRA, TSP, SMP (Symmetric Multiprocessing) and multicore.

In plain words, MORA-IMA will combine for the first time ESA's three major technological goals concerning Embedded Space Software. It will achieve an end-to-end process starting from high-level software design, passing through a full avionics-, system- and software-architecture using the OSRA process and finishing up with automatic code generation, build and execution on a multi-core space computer applying the IMA/TSP paradigm.

The elected use case for this study is ESA´s EagleEye Reference Mission. EagleEye is ESA's virtual space mission for software testing; it has been and is being used to try out and evaluate methods, technologies, and tools for space mission development. EagleEye includes a full Software Validation Facility (SVF) and Central Software (CSW) of a satellite, properly installed on ESA´s Avionics Test Bed (ATB).

Eutelsat entrusts GMV with its next four missions

EUTELSAT HAS ONCE MORE TURNED TO GMV, IN THIS CASE FOR IMPLEMENTATION OF THE CONTROL CENTER (NEO-SCC), THE EUTELSAT VERSION OF GMV'S ***hifly®*** PRODUCT, PLUS THE ***focusGEO***-BASED FLIGHT DYNAMIC SYSTEM FOR ITS NEXT FOUR MISSIONS

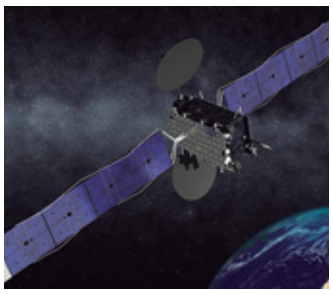
Eutelsat is now one of GMV's flagship clients, running GMV-developed systems for controlling its whole satellite fleet, pride of place going to the multi-satellite control system ***hifly®*** and the flight dynamics system ***focusGEO***.

The long-lasting and solid relation between GMV and Eutelsat, dating back to the first contract award in 1993, has been forged largely by a great 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.

Avant Project, as the project has been called, represents the first GMV development for Eutelsat involving the almost simultaneous implementation of four new satellites. This poses a stiff challenge at both technical and managerial level, for which GMV will draw on synergies from other inhouse GMV developments of both the ***focus*** and ***hifly®*** families. The project's roadmap also provides for the use of agile development methodologies with the goal of ensuring the best use of GMV resources and to guarantee fulfilment of Eutelsat's operational, functional and quality goals.

Avant Project will run up to early 2019 and support Eutelsat operations for the following four satellites:

African broadband broadband satellite of Thales Alenia Space based on the new Spacebus Neo platform. Like Quantum, it provides a telemetry and telecommand transmission protocol based on ESA's Packet Utilisation Standard (PUS). This African broadband satellite is to be launched in 2019.



Eutelsat 5 West B, the first Eutelsat satellite of the manufacturer Orbital ATK with a GeoStar2 platform and an Airbus Defence and Space payload. Also to be launched in 2018.

Eutelsat Quantum of the manufacturer Airbus Defence and Space (ADS) in the UK with a platform made by its subsidiary Surrey Satellite Technology Ltd. (SSTL). Quatum is the first satellite to allow complete onboard reconfiguration.

Eutelsat 7C built on Space Systems Loral's Omega 3 platform, due to be launched in Q3 of 2018 to give broadband coverage to Europe, Africa, the Middle East and Turkey.

Start of the operational phase of the HISPASAT AG1

On 2 June, after completion of the commissioning phase, the Hispasat 36W-1 (AG1) satellite was officially handed over to the operations team, a watershed moment that marks the start of the satellite's operational life.

Launched on 28 January, Hispasat AG1 is the first mission of the SmallGEO platform developed by OHB System AG (Germany) with the European Space Agency and HISPASAT. The satellite features the innovative RedSAT regenerative payload, which will allow HISPASAT to use the satellite's power more flexibly and efficiently, significantly boosting its transmission capability with the concomitant reduction of communications costs.

To support the 20 Ku-band transponders and up to 3 Ka-band transponders, GMV has supplied Hispasat not only with a groundbreaking active antenna with reconfigurable beams but also the latest version of its Smart family of tools: ***smart rings*** and ***smart beams***. The former seeks payload configuration alternatives in the event of any component failure and the latter offers the user total control over antenna alignment configuration while also showing a 3D map of the antenna boresight for checking purposes.

Both tools are fully integrated with the multi-satellite control and monitoring system, ***hifly®***, and with the flight dynamics system, ***focusGEO***, both supplied by GMV. For this satellite, moreover, ***hifly®*** has incorporated support for ESA's new telemetry and telecommand protocol called Packet Utilisation Standard (PUS), already being phased into the new satellite models by other manufacturers.

HELLAS SAT 3 successfully launched

On 29 June a European Ariane 5 rocket blasted off from the Kourou spaceport to place in orbit the new telecommunications satellite of the Hellas Sat fleet, a subsidiary of Arabsat.

Hellas Sat 3, a shared satellite between Hellas Sat and Inmarsat, will carry out two missions: Inmarsat will deploy an integrated satellite and ground network that will deliver robust, high capacity inflight broadband for airline passengers across Europe, while Hellasat will offer Direct-to-Home (DTH) television and Telecom services to Europe, the Middle East and North Africa, substituting and enlarging the capabilities of its forerunner, Hellas Sat 2, which is now reaching the end of its useful life.

GMV has developed the Hellas Sat 3 flight dynamics system and monitoring and control system. Both these systems have been developed from GMV's inhouse ***focusGEO*** and ***hifly®*** solutions, and have been successfully integrated and deployed in a modern and environmentally-friendly virtual environment using blade and vSphere servers. As well as the software, GMV is also providing training, support and maintenance for the system's end users.

The launch and operational commissioning of this satellite represent further success in the development of both satellite-control systems.

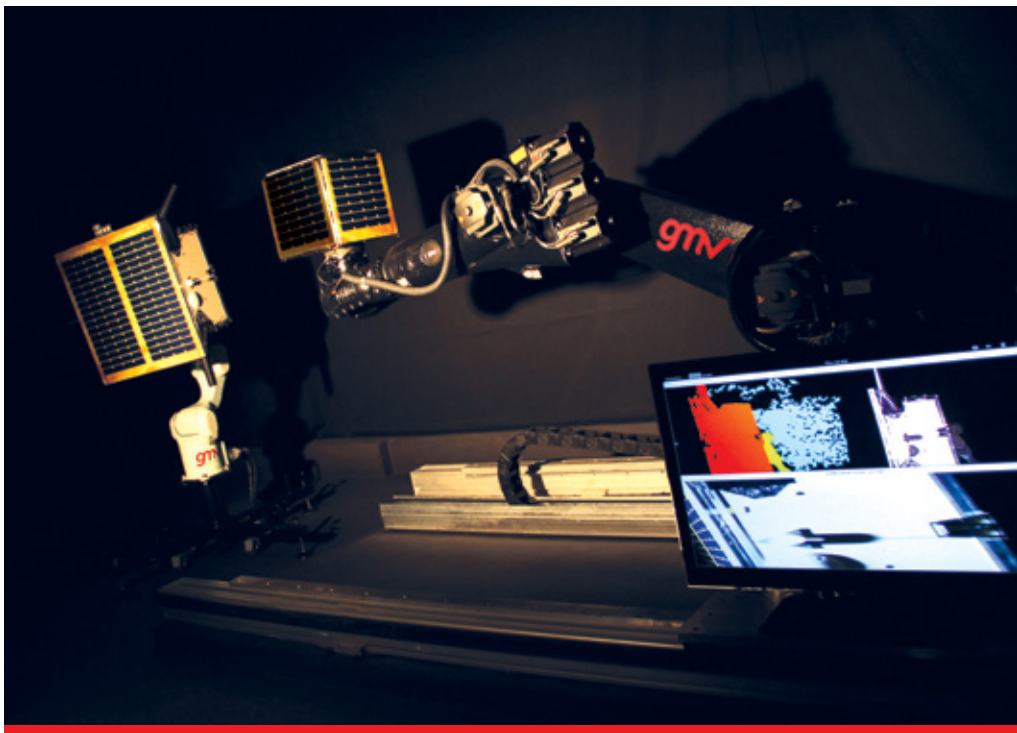
GMV is working to defend the planet from asteroid thread

IT IS NOW CRUCIAL FOR OUR SOCIETY TO COMPREHEND THE REAL THREAT POSED TO OUR PLANET BY ASTEROID STRIKE, ESPECIALLY IN LIGHT OF ITS INCREASING COMMUNICATIONS- AND TECHNOLOGY-DEPENDENCE. WE URGENTLY NEED TO COME UP WITH A REMEDY FOR THIS THREAT

Planetary defense calls for the development of technologies such as Guidance, Navigation and Control (GNC) of spacecraft in the vicinity of asteroids. This allows us to carry out missions to study the characteristics of asteroids and deviate them by impact if need be.

GMV has been actively working on projects of this type for years now. AIM (Asteroid Impact Mission), as part of the AIDA program (Asteroid Impact and Deflection Assessment), aims to study the effect of the impact of the NASA DART probe against the moon of the Dydimos asteroid, while also demonstrating new optical communication technologies in space as well as studying and characterizing the internal and surface structure of Didymos and its moon; FCS ATOMIC (Flight Control System Assessment Toolbox for Optimal Mission Cost and Performance) is a GMV-led initiative that sets out to establish a real framework for a Flight Control System (FCS) made up by FDS and GNC systems plus their corresponding interfaces to weigh up the feasibility of future missions. Last but not least, TAIM (Asteroid Impact Mission Thermal Infrared Imager) is the name given to a study focusing on the development of a thermal imaging camera to capture images in the infrared spectrum for ESA's Asteroid Impact Mission (AIM).

During this year GMV has also been actively participating in the European Commission's asteroid-strike planetary defense project, NEOShield-2 . This 4.2- million-euro project, which kicked off back in 2015, is an EU H2020 R&D initiative primed by Airbus Defense and Space GmbH and involving 11 other European firms.



GMV's Advanced Robotic Testbed ***platform-art©***

NEOShield-2 is developing the necessary space-mission technology to divert threatening asteroids. The project also studies how to measure deviation attempts with precision and how to carry out in situ analyses. Studies are now being made of astronomical observations, modeling, simulations and the physical characterization of near earth objects (NEOs) in order to gain a better understanding of their physical properties. Lastly, work is underway on drawing up a European strategy for future mission-associated research activities.

Within NEOShield 2 GMV has taken on the development of the autonomous guidance, navigation and control (GNC) system based on artificial vision for landing the spacecraft on the asteroid, collecting samples weighing at least 30 grams and returning them to earth. This type of mission is crucial for accurately studying the asteroid's features before deflecting it. GMV is also developing and running testbeds for ground validation of the NEOShield-2 consortium's 3 GNC systems, namely the Optical Navigation Testbed and GMV's inhouse Advanced Robotic Testbed ***platform-art©***. These two between them allow ground simulation of space-scenario conditions and real time stimulation of the spacecraft's onboard computers and sensors.

GMV showcases its latest ADR breakthroughs

GMV SHOWCASES ITS ADR BREAKTHROUGHS AT THE EUROPEAN CONFERENCE FOR AERONAUTICS AND SPACE SCIENCES, EUCASS 2017

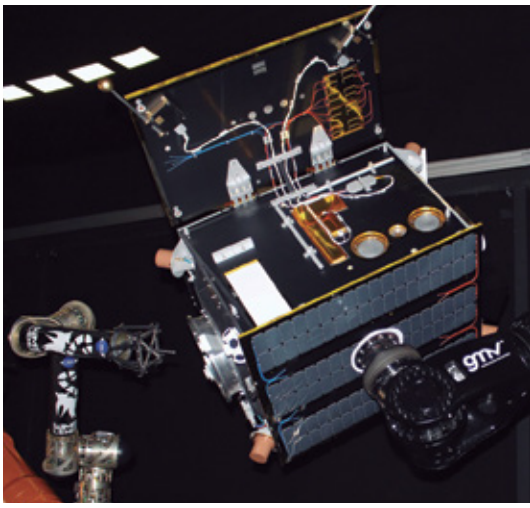
From 3 to 7 July GMV took part in the 7th European Conference for Aeronautics and Space Sciences, EUCASS 2017. To showcase its latest ADR (Active Debris Removal) breakthroughs, it presented the results of three projects it is carrying out for the European Space Agency.

The first of them, SBSS-DM, aims to demonstrate the objectives of the SBSS mission (Space-Based Space Surveillance), concentrating on surveillance and monitoring not only of artificial objects but also near-earth objects (NEOs).

The second of the presented research projects was AnDRoID, part of the IOD (in Orbit Demonstration) project, which is focusing on the capture of small space-debris objects (100-200kg).

Lastly, the ORCO project (On Ground Validation of a Rigid Combo system), aims to perform ground consolidation, integration and validation of the key technologies for carrying out complex space robotics initiatives (based on Active Debris Removal for a small satellite).

EUCASS, held since 2005, is one of Europe's main scientific aeronautics and space events, always attracting a healthy turnout of scientists, researchers and stakeholders not only from Europe but also from Asia and America.



The ORCO project aims to perform ground consolidation, integration and validation of the key technologies for carrying out complex space robotics initiatives

GMV previews the Copernicus program's observation requirements for agriculture

GMV took part in the Conference on Copernicus Applications for Farming put on by the Ministry of Agriculture, Fisheries, Food and the Environment (*Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente*) on 11 May in Seville, with the collaboration of the Industrial Technology Development Center (CDTI) and the Regional Authority of Andalusia (*Junta de Andalucía*).

Julia Yagüe, GMV's Copernicus Services Manager, took part in the panel discussion "Opportunities for Spanish industry and public research organizations"

This conference is part of the ongoing effort to bring the European Commission's Copernicus program to wider notice in Spain. It focused on the beneficial use of the European Copernicus program's satellite data for monitoring the state of the environment and agriculture.

GMV is currently leading the European Commission framework program which sets out to define user requirements for the future generation of Copernicus satellites, by means of which Europe is now building up its own earth observation capability.

The user requirement database now has nearly 4000 records referring to the six thematic areas of Copernicus, namely atmosphere monitoring, marine monitoring, land monitoring, climate change, emergency management and security.

GMV also announced the Commission's interest in extending the requirements study for the design of Copernicus's future space component to take in such across-the-board areas as agriculture, water resources, cultural heritage, insurance and tourism.

GMV and Thales sign a contract for development of the new generation of EGNOS's CPFPS

On 16 June 2017, after a year-and-a-half of negotiations, GMV and Thales Alenia Space France signed a ten-million-euro contract for developing the new generation of CPFPS (Central Processing Facility- Processing Set), also known as CPFPS-G2. This is GMV's main contribution to the future version of EGNOS V2.4.2, which is expected to be certified and declared operational by the end of 2019.

EGNOS (European Geostationary Navigation Overlay Service) is Europe's satellite-based augmentation system (SBAS) that is used to improve the performance of traditional global navigation satellite systems (GNSSs) such as GPS and GLONASS. Over the years GMV has played a vital role in this European SBAS, working on it since its initial phases in 1995. Since then, among other activities, GMV has participated in the development of the CPFPS, the critical software item and heart of the message-generating system with the corrections to be used by the end user.

It has also worked on development of other elements at operational level such as the ASQF (Application Specific Qualification Facility), used as support for qualification of EGNOS applications, or on engineering components such as the EETES (EGNOS End to End Simulator), which has been in operation since 1999 to generate the reference scenarios used afterwards during subsystem and final-system validation phases.

The CPFPS currently deployed, providing corrections as part of the EGNOS message, has been drawing on technology dating right back to 1999, both in terms of the operating system (RTOS) and the hardware. This infrastructure has been obsolete for several years now and is becoming increasingly difficult to maintain. Nonetheless, GMV, by means of the current maintenance service contract (CPFPS_PSS), guarantees problem-free maintenance of the current CPFPS up to 2021.

But the obsolescence problem won't go away of its own accord; it calls for development of a new CPFPS with new hardware and software. For this reason the decision was taken to solve the obsolescence problem once and for all and set up a new system by late 2019.

From 2014 to 2015 GMV carried out the preliminary design phase, selecting both the hardware and operating system for the new generation of CPFPS. This selection was done on the basis of ESA's diversification and homogenization requirements.

Midway through this year, after conclusion of the negotiations to fine-tune both the timetable and the scope of the activities to be carried out, GMV and Thales Alenia Space–France signed the contract for developing the new CPFPS generation, thus assuring EGNOS V2 service provision for at least another 15 years.

But it doesn't stop there. Important mid-term algorithmic improvements are to be phased in together with mission requirements such as transmission of GPS-like correction signals from GEO satellites or "GEO ranging", exploiting the existence of this new CPFPS subsystem with a more modern and efficient infrastructure.

Project Team

GMV has played a vital role in this European SBAS, working on it since its initial phases in 1995

GMV leads ESA's project to help to manage the migration crisis through Satellite Based Technology

According to the International Organization for Migration (IOM), the number of migrants and refugees that have crossed into Europe by sea has soared in recent times. Thousands of people have died while looking for better living conditions.

Mindul of this situation, the European Space Agency (ESA) has awarded a study to GMV with the goal of characterizing big data space-based services to support identification of human migration flows, assessing their technical feasibility and viability, and proposing a roadmap for their implementation and sustainable exploitation.

Together with key stakeholders, GMV UK supported by GMV Portugal is leading this feasibility study that will assess requirements from international entities such as the International Organization for Migration (IOM), Frontex, SatCen and EASO but also from other players such as NGOs (*Conselho Português para os Refugiados, AMI, Ayuda en Acción*) and local law-enforcement entities.

This project integrates multiple space assets (Satellite Imagery, GPS data used for geo-localization, satellite communications etc.); "Big Data" sources, either terrestrial or derived from space assets (call data records, social media data, earth observation data etc.); and focuses on the three identified emergency-management phases (mitigation, preparedness and response).

This study will assess the added value of big data solutions in the migration sector, namely the reduction of safety risks for migrants, the enhancement of border controls, as well as prevention and response to security issues related with unexpected migrations movements. Additionally, the feasibility study provides insights from people involved in migration; these insights will then help to understand the migration phenomenon better while also enhancing efficiency in the integration and assistance of migrants.

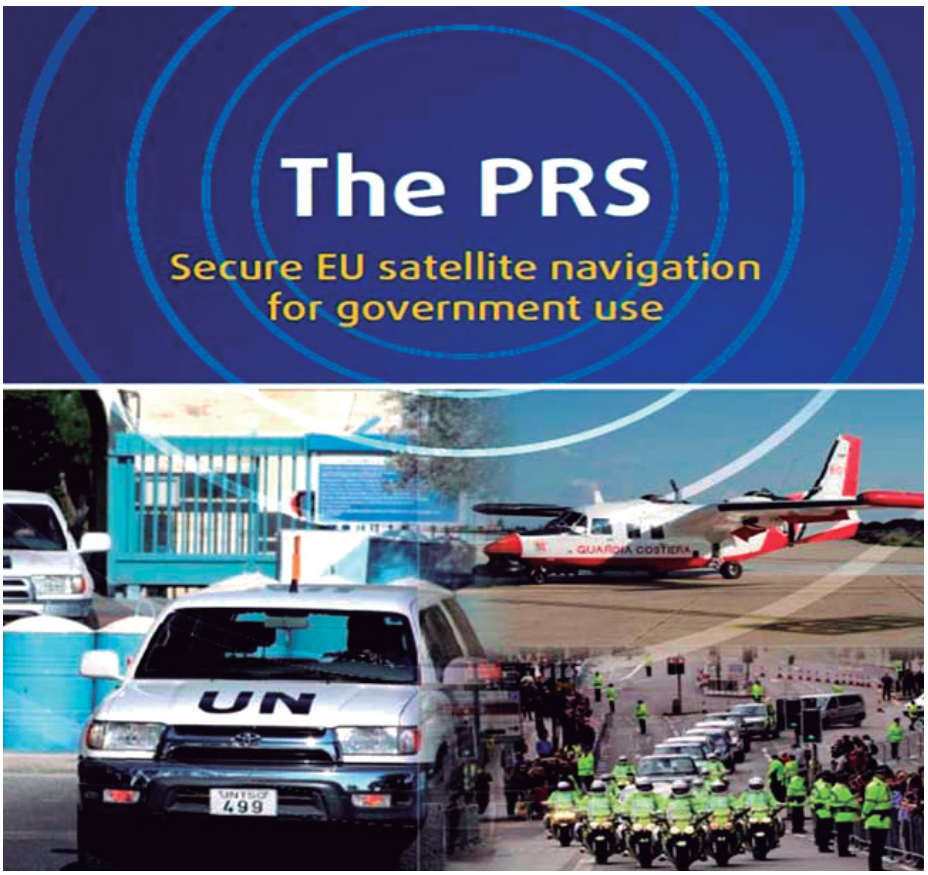
Once again, Big Data technologies have a crucial role to play in providing information on human migration and movements by tapping into several space assets (Earth Observation imagery, Satellite Communications or Global Navigation Satellite Systems) and integrating them with other terrestrial assets (cell-phone records, social media data etc.).

GMV attends Portugal's science and technology meeting

GMV was one of the invited companies of encontro Ciência'17, an annual meeting of the Portuguese science and technology community. It aims to promote an open debate on the main subjects and challenges driving the work of Portugal's science community.

Teresa Ferreira, Director of Space in GMV Portugal, took part in the session "Portugal Space 2030: Satellites, Antennas and Launchers", where she stressed the importance of raising the national industry's technology maturity level and encouraging international cooperation.

Ciência 2017 is an annual meeting brokered by the Ministry of Science, Technology and Higher Education, and organized by *Fundação para a Ciência e Tecnologia* in collaboration with *Ciência Viva - Agência Nacional para a Cultura Científica*, and the Education and Science Parliament Committee.



GMV paves the way for better PRS signal processing

THE EUROPEAN SPACE AGENCY HAS ONCE AGAIN TURNED TO GMV IN PORTUGAL FOR THE STUDY OF SIGNAL PROCESSING TECHNIQUES TO PROCESS HIGHER ORDER BINARY OFFSET CARRIER MODULATIONS SUCH AS THE ONES USED BY THE GALILEO PUBLIC REGULATED SERVICE (PRS)

In this activity, GMV together with Tampere University of Finland and *Universitat Autònoma de Barcelona*, have pushed back the limits of state-of-the-art techniques and characterized their performance. This knowhow will be of the utmost importance in the near future since the speedup in Galileo deployment and the new PRS service will require a new category of receivers capable of exploiting the signal features. The PRS is an encrypted navigation service for governmental authorized users and sensitive applications that require high continuity. This work has led to articles in IEEE Signal Processing Magazine and in this year's ION, one of the most highly esteemed GNSS Conferences.

This knowledge has been materialized in GMV's PRS receiver that will be used under operational scenarios aiming at demonstrating the added value of such a service while consolidating GMV's position in the landscape of PRS receiver providers.

GMV becomes a member company of Eurospace

IN KEEPING WITH ITS PROVEN LEADERSHIP IN THE SPACE SECTOR, GMV HAS RECENTLY JOINED EUROSPACE, A PROFESSIONAL ASSOCIATION SET UP IN 1961 AS THE EUROPEAN NON-PROFIT ORGANIZATION TO BRING TOGETHER EUROPE'S ENTIRE SPACE INDUSTRY

Eurospace's remit is to foster the development of space activities in Europe and promote a better understanding of the sector's issues and problems. It gathers sector-relevant information and keeps up permanent liaison with ESA (the European Space Agency), National Space Agencies and, in general, any organization using or promoting the use of space techniques, such as the various European governments or the European Union.

GMV joins Eurospace with the aim of inputting its almost 35-year experience and expertise in the space sector and helping to drive initiatives that boost Europe's space industry, generating valuable employment and collaborating in the carrying out of cutting-edge hi-tech projects.

Eurospace membership covers 14 European countries. Together they represent more than 90% of the total European industrial turnover in space activities. This makes Eurospace the most representative association of the space industry in Europe.

Thales Alenia Space-Italy takes up GMV's mission planning system for the second generation of COSMO-SkyMed satellites

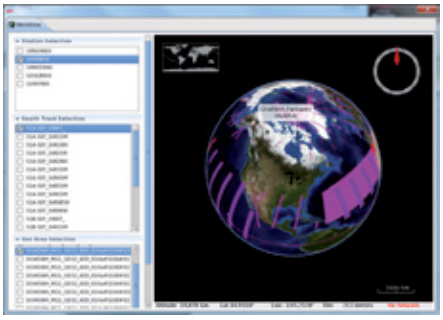
In 2016 Thales Alenia Space was chosen by the Italian Space Agency (*Agenzia Spaziale Italiana: ASI*) to prime development of the program called COSMO-SkyMed (COnstellation of small Satellites for the Mediterranean basin Observation) Second Generation, which includes a two-satellite constellation for dual military and civil use. Each satellite comprises a Synthetic Aperture Radar (SAR) for taking earth-observation images.

GMV's inhouse mission-planning system, ***flexplan***, has recently been acquired by Thales Alenia Space to be evaluated as the mission-planning system for this second generation of earth-observation satellites. ***flexplan*** uses an algorithm generator that allows flight and mission rules to be implemented, changed and vetted without recompilation. Due to this flexibility, it can be used for any type of mission (interplanetary or terrestrial orbit) and can be configured, deployed and integrated swiftly in the mission's ground segment.

flexplan is an operational system already being used in missions similar to this program such as Sentinel-1, within the European Commission's two-satellite Copernicus program, whose payload also comprises SAR instrumentation, or the PAZ satellite, which forms part of Spain's National Earth-Observation Program (*Programa Nacional de Observación de la Tierra*: PNOTS) and is slated for launch and commencement of operations by the end of this year.

This new acquisition means ***flexplan*** has now been taken up by yet another national space agency, to be added to the longstanding clients of ESA, NASA, EUMETSAT and the Korean Space Agency, among others.

flexplan *Schedule Generation Human-Machine Interface*



flexplan *3D display of World Map Visualizer*

The UK Space Conference brings together the whole space sector

GMV AS SUCH IT DID NOT WANT TO MISS THIS FLAGSHIP EVENT, THIS YEAR, FROM 30 MAY TO 1 JUNE, CAME THE TURN OF MANCHESTER

At this latest UK Space Conference GMV showcased its current range of space-segment services and products (guidance, navigation and control systems) as well as its ground-segment developments (telecommunication-satellite control centers, earth-observation-mission data processing systems and applications using space technologies and data) and its inhouse robotics developments.

GMV also wished to shine a particular spotlight on the areas actually run from the British subsidiary and the projects it is currently carrying out. Within the robotics area GMV is participating in the HRAF (Harwell Robotics and Autonomy Facility) development as well as in ERGO (European Robotic Goal-Oriented autonomous controller) within the European Peraspera framework. In the earth-observation area GMV is developing processing components for ESA's EarthCare mission as well as satellite-data applications as support for mining, agriculture and migratory crises.

The UK Space Conference is one of the world's biggest and finest space events, three days of immersion and networking, bringing together government, industry, academia, customers, suppliers, education providers, researchers, etc, to swap ideas and compare notes on the space community's latest breakthroughs, technological developments and innovations, while exchanging views on how this knowledge might bring about changes of a social, political and economic nature.

GMV provides critical technology for the Phobos Sample Return mission

GMV IS PRIMING THE CONSORTIUM FOR DEVELOPMENT OF THE VISION BASED NAVIGATION CAMERA (VBNC) WITHIN THE PHOBOS SAMPLE RETURN MISSION

GMV's current contract with the European Space Agency consists of providing an Engineering Model (EM) of high-performance avionics for processing navigation images by means of feature extraction algorithms and looking for matches between continuous images of the surface of Phobos, the moon closest to Mars.

The purpose of the Phobos Sample Return Mission, within the Mars Robotic Exploration Preparation (MREP-2) program, is to bring soil samples from the Phobos satellite back to the Earth. This is considered to be a mid-term milestone towards the long-term objective of developing the critical technology required for the Mars sample return mission. Within this mission GMV is developing a Guidance, Navigation and Control (GNC) system for the landing phase, using image-based autonomous navigation techniques.

As well as the image-processing engineering model, another component being developed within this project is the Camera Optical Unit (COU), comprising the lenses, detector and image-preprocessing and acquisition avionics. The optical unit is built into the Image Processing Board (IPB), which in turn connects up to the flight computer running the GNC navigation filters. The selection of the avionics of these systems, and implementation of image-processing algorithms in said avionics will enable runtimes to be reduced by between tenths of seconds to hundredths of milliseconds; this is crucial for a rapid landing dynamic.

The purpose of the Phobos Sample Return Mission, within the Mars Robotic Exploration Preparation (MREP-2) program, is to bring soil samples from the Phobos satellite back to the Earth

Last May saw successful accomplishment of the preliminary design review in which GMV presented the architecture design of the Image Processing Board and the Camera Optical Unit subsystems of the VBNC with the interconnection of all components. The architecture includes components capable of withstanding mission conditions, centering on the Martian environment, and a fault-tolerant design including redundant systems. As validation of the whole system, GMV also presented the ground support hardware; this includes the flight computer, for which a quad-core Leon4 with RTEMS has been chosen as the real-time operating system.

Lastly, a preliminary validation and verification plan was presented, taking in the full life-cycle process from unit testing to system tests, at functional, electrical and environment levels.

GMV invited to ESA's Earth Observation seminar

Earth Observation (EO) technologies are constantly evolving, as well as the way we process and exploit satellite data. The scientific, societal and economic benefits of this data are virtually endless, and realizing their full potential in these three areas is crucial.

With this situation in mind, on 11 May the European Space Agency (ESA) held in ESRIN an invitation-only seminar to address this sector's paradigm switches and prospects over the coming years. The guests included representatives from all national delegations plus the main international companies of the sector, ranging from commercial satellite providers and operators, like Planet and SSTL, to cloud technology providers like Google Earth, Amazon Web Services and Microsoft.

The ceremony, hosted by ESA's Director of Earth Observation Josef Aschbacher, tackled such burning issues as microsatellite constellations; cloud computing, Big Data and Internet of Things; open data policies or how to make sure the public at large can benefit from EO data.
GMV, a benchmark earth-observation company, was invited to participate as part of both the Portuguese and Spanish representations, the latter brokered by the Industrial Technology Development Center (*Centro de Desarrollo Tecnológico Industrial*: CDTI). Leading figures at the seminar included Luis Mariano González Casillas, director of the applications- and payload-data-processing business unit, and Teresa G. Ferreira, Space Director in Portugal.

Notably, GMV was the only Spanish guest, largely on the strength of its designation by the European Commission as Spain's Copernicus link.

GMV takes part in the international summit "Atlantic Interactions"

International Research Center for the Atlantic constituded in Azores by the end of 2018

The island of Terceira in the Azores was the venue for the international "Atlantic Interactions" summit attended by government representatives, companies and scientific and academic institutions from 29 countries, as well as delegations from the European Space Agency, the European Commission and the European Parliament, and the United Nations. Representing GMV was the General Manager of Portugal, Alberto de Pedro Crespo.

The main objective of the summit was to prepare the creation of the Atlantic International Research Center (AIR Center) in the Azores, a research center focused on the study of the Atlantic, in the areas of space, climate change and the atmosphere, renewable energy and data processing.

As part of this summit, Manuel Heitor, Minister of Science, Technology and Higher Education of Portugal, announced the creation of the International Research Center for the Atlantic of the Azores by the end of 2018.

A new November summit is scheduled to take place in Brazil and aims to validate the commitments now assumed.

Urban GreenUp kicks off, an H2020 project to renature cities

ON 7 JUNE VALLADOLID (SPAIN) HOSTED THE OFFICIAL LAUNCH OF THE URBAN GREENUP PROJECT, FUNDED UNDER THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAM. ITS AIM IS TO DEVELOP A NEW STRATEGY FOR RE-NATURING CITIES THROUGH NATURE-BASED SOLUTIONS

Presentation of Urban Green Up project

Apart from the environmental benefits of projects of this type, such as increasing resilience to climate change and making cities healthier to live in, the project also aims to drive the green economy within the urban environment, creating jobs and new opportunities and business models. As well as technical actions the project also includes educational activities with public participation and activities to raise city dwellers' awareness about the environmental, economic and social benefits of green infrastructure.

Urban GreenUp, working with a total budget of 14.81 million euros, is being coordinated by the CARTIF Technology Centre and carried out by a wide-ranging international consortium of 25 partners from 9 different countries from 3 continents.

In Spain the Ayuntamiento (City Council) of Valladolid, through its Economic Development and Innovation Agency and with the collaboration of the regional ministries of town-planning and the environment, the River Duero Water Board (*Confederación Hidrográfica del Duero*), the technology centers CENTA and LEITAT and the companies Acciona, Singular Green and GMV, will be responsible for carrying out the planned project activities in the city of Valladolid itself. Together with Esmirna (Turkey) and Liverpool (UK) Valladolid is one of the project's three demonstrator cities.

Activities to be carried out in Valladolid include green roofs and facades, vertical mobile gardens, permeable pavements, green noise barriers, smart soils that reduce watering and fertilizer needs and a floodable park alongside the River Esgueva as an example of its flood-damage reduction potential for a flood-prone city like Valladolid.

Within this project GMV is responsible for the work package to monitor renaturing measures. Its final aim is to establish a monitoring scheme to gauge the impact of such measures in terms of improving cities' response to the abovementioned challenges (e.g. climate change). This will provide a robust data-driven, evidence-based monitoring and diagnosis scheme.

To this end GMV, together with its Urban GreenUP partners, will be helping cities to define and implement a series of key Performance Indicators (KPIs) and will define an ICT platform that is compatible with the cities' current working protocols and tools. The various project partners will be inputting a series of in situ, airborne and satellite sensors that will measure the parameters over several years in order to calculate the most suitable efficiency indicators for each renaturing measure. After this monitoring period a global evaluation will then be made of the results in each city.

GMV will also develop a smartphone application to encourage environmentally-friendly behavior in citizens. The smartphone application will score different aspects of end-users' activity and lifestyle (sustainable mobility, energy-saving, renewable energy, third-party dissemination. etc.) aligned with the defined KPIs and also an overall combined score. To promote end-user participation, the app will also offer periodic scoreboards and support events, with the idea of rewarding users according to their "green-rating".

The project such as increasing resilience to climate change and making cities healthier to live in, creating jobs and new opportunities and business models

GMV puts the LUCID rover through its paces

LUCID (LUNAR SCENARIO CONCEPT VALIDATION AND DEMONSTRATION) IS A GMV-LED EUROPEAN SPACE AGENCY (ESA) PROJECT THAT SETS OUT TO EVALUATE THE COMBINATION OF NECESSARY TECHNIQUES AND TOOLS FOR OPERATING A LUNAR PROSPECTOR ROVER (LPR) EFFICIENTLY AND SAFELY WITHIN THE ENVIRONMENTAL AND OPERATIONAL CONSTRAINTS OF THE LUNAR POLAR REGION

Within this project GMV has installed system equipment and developed the rover's software.

During this year LUCID is being put through its paces in Madrid and Tenerife to check that all the LPR's systems work properly.

Fernando Gandía, head of the LUCID project, tells us about these tests and how they are being conducted.

How many tests will be carried out within the whole project?
After the two weeks of preliminary tests in the area known as Dehesa de Navalvillar near Madrid in Colmenar Viejo, another four weeks of tests have been scheduled in Minas de San José in the National Park of Teide on the Canary Island of Tenerife, of which the first two weeks have now been completed. In autumn we will be going back to Tenerife to complete the final two weeks of tests, involving experiments lasting over two hours and very similar to the operation of a real mission.

What do they consist of?
The main aim of these trials is to assess different combinations of tracking and situational awareness techniques. This will give future operators of LVP-like robotic missions a much more complete and reliable picture of the environment through which the rover is moving. In this particular case we are concentrating on techniques especially designed to withstand the constraints and tricky lighting conditions of the lunar poles.

Does the choice of these test sites respond to any overall goal?
On our planet there is no perfect match for the lunar poles. Nonetheless, there are certain regions that could be considered to be lunar analogs from various points of view. In particular the area known as Cañadas del Teide is a fairly close match in terms of the general lithology of the terrain and the structure and makeup of the regolith (the decomposed material forming the soil over which the rover moves). This makes them a good terrain analog for what we might find inside the moon's craters. The Island of Tenerife is also very convenient from a logistic point of view.

Why is it so important to carry out different tests within the project?
The tests are crucial for several reasons. First and foremost, they are the best way of effectively validating the human/machine interaction, i.e., evaluating whether the information supplied by all techniques in real conditions is sufficient for the rover operator and whether this information is offered in the best way possible. Secondly, the tests are essential in terms of increasing the system's maturity and reliability by confronting it with the most realistic possible working conditions.

Pending the final tests, have any conclusions been drawn yet?
Although it's a little early to venture any result, we can safely claim that the first part of the test campaign has

been a success. All tests planned for the first two- week stay on Tenerife were actually carried out. Throughout this time we managed to operate the rover remotely with no sightline from the operator and in total darkness over tricky terrain. These tests have given us priceless information on the specific usefulness of each one of the techniques used and the best way for the operator to make use of them according to the terrain being crossed by the rover. During the second part of the test campaign we will be operating in even more difficult conditions (longer runs over more complicated ground). We will also be weighing up the usefulness of the same techniques in an autonomy scenario, in which the rover has to be capable of executing complex plans drawn up by an operation team from information received.

Will we be seeing LUCID on the moon in the near future?

The Field Test Rover (FTR) being used on the LUCID project is a demonstrator built up from equipment of terrestrial use and, as such, unfit for space travel. Nonetheless, the design teams of missions like LVP are awaiting the LUCID analysis results with great expectation. This feedback will help them take decisions of vital importance in terms of the choice of sensors and technology to be developed and assembled in the rover that actually will make the trip to the moon.

As well as the LUCID project, GMV is also leading other European Commission H2020 space robotics projects: the European Space Robotics Control and Operating System (ESROCOS project); the European Robotic Goal-Oriented Autonomous Controller (ERGO project); coordination of the testing phase of the two former projects and others in diverse European laboratories (FACILITATORS project)

LUCID project team in the National Park of Teide

Robdos Team heads for the ERL Emergency Competition

The team has been working since 2016 on its own autonomous underwater robot. The end in view is the ERL Emergency Robots 2017 competition. This competition poses a grand challenge involving realistic, multi-domain emergency-response scenarios that can only be overcome if land, underwater and flying robots successfully cooperate in evaluating the environment, compiling information and identifying possible dangers.

Robdos Team is the name of the team that GMV has been backing since 2016. Its 13 members come from different fields.

In 2016 the team set out to develop its own inhouse robot, WASABI (Water-resistant Autonomous System for Assistance, Bathymetry and Inspection), thanks to sponsors like GMV. The first step was the construction of a prototype platform, a testing catamaran, to be able to work simultaneously on construction and programming.

All this spadework has now resulted in a modular autonomous robot they have been working with since early 2017. This robot is capable of taking up different configurations to suit the particular activity to be carried out in each case.

Robdos Team is currently putting the final touches to their preparations for the European Robotic League (ERL) Emergency competition, to be held from 15 to 23 September 2017 in Piombino, Italy, under the auspices of the University of the West of England (Bristol).

The end of the ARGOS Challenge, TOTAL's R&D initiative

TOTAL, the world's 4th biggest oil & gas supplier, organized the ARGOS Challenge together with the French National Research Agency (ANR) with the aim of bringing robotics and industry closer together and demonstrating its technological innovation capacity. The remit of the competition was to design, develop and validate an autonomous surface robot to work on oil and gas sites, capable of inspecting and monitoring the industrial environment, pinpointing any anomalies and intervening in emergency situations.

This is the first time this challenge has been held and the overall results matched the quality of its participants. Over three years of thrilling trials only five teams actually pitted their wits against all three rounds of the challenge.

GMV was one of these shortlisted teams from the thirty applicants, leading the FOXIRIS team, together with IDMind (a Portuguese industrial robotics manufacturer specializing in locomotion platforms) and UPM-CAR (the Automation and Robotics Center of Madrid Polytechnic University - *Universidad Politécnica de Madrid*).

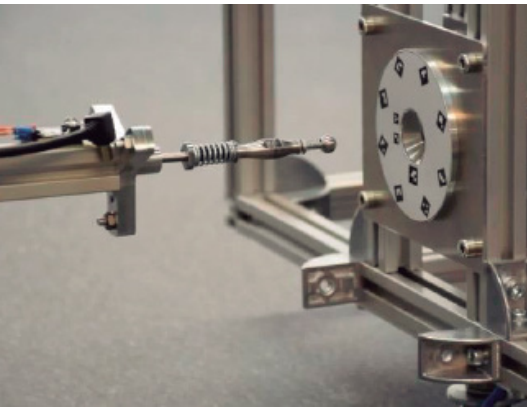
AIR-K (Japan), ARGONAUTS (Austria and Germany), LIO (Switzerland) and VIKINGS (France) were GMV´s rivals in the competition site of Lacq in southern France. After each round of the competition, held in June 2015, April 2016 and March 2017, the international jury issued a technical report with various recommendations for each team while also updating the assessment criteria for the trials of the next round.

The curtain was finally brought down on the ARGOS Challenge by the prize-giving ceremony held on 11 May 2017 in Total's Tour Coupole in Paris. This was a thrilling and emotion-packed recapitulation of the key events during the three years of the competition, culminating with the award of the trophies to the winning team, the ARGONAUTS, and the rest of the participants, FOXIRIS, LIO, VIKINGS and AIR-K.

GMV was one of these shortlisted teams from the thirty applicants, leading the FOXIRIS team, together with IDMind and UPM-CAR

Robot technology for space-debris removal and refueling missions

IN MAY 2017 THE COMRADE (CONTROL AND MANAGEMENT OF ROBOTICS ACTIVE DEBRIS REMOVAL) KICK-OFF MEETING TOOK PLACE



The purpose of the two-year project is to design, develop and test the control system of a robotic S/C (including manipulator and end-effector) for two types of mission: an Active Debris Removal (ADR) mission and a refueling mission, taking their cue, respectively from the ASSIST mission and the eDeorbit mission.

GMV is leading a team comprising all the following: ADS, who will provide the necessary expertise on space missions system level, DLR, which will input its almost unique space-robotics expertise; Bordeaux University, which will be responsible for the robust control implementation; NTUA-CSL, which will input its ASSIST experience, including the set-up and test of the ASSIST scenario on its air-bearing test bench; and lastly PIAP, which will make its gripping mechanism available to the project, designed for ADR purposes and more specifically the e.Deorbit mission.

The meeting laid down the main project goals and clarified the first steps to be taken towards them.

GMV strengthens its position in the international defense and security market

IN 2016 GMV CHALKED UP RECORD SECURITY AND DEFENSE SALES. THIS IS UNDOUBTEDLY AN EYECATCHING FEAT IN A CONTEXT OF WORLDWIDE ECONOMIC DOWNTURN, BUDGET-CUTTING AND UNCERTAINTY

This milestone endorses GMV's position as an international security and defense benchmark. This position rests on three main pillars: firstly, direct contracting with European agencies; secondly its sales of JISR products (Joint Intelligence Surveillance and Reconnaissance) and thirdly the company's participation in R&D programs such as the European Horizon 2020.

GMV now has a longstanding track record of cooperation with international agencies on the strength of contracts won in tenders of open competition. It has been collaborating with the European Defense Agency (EDA) since its creation in 2004. Under the Joint Investment Program in Force Protection GMV was the only European country to win two contracts. With EDA the company has forged even closer bonds in recent years and it is now working for the agency in such important areas as Cyberdefense, C2 systems for dismounted soldier and federated mission networks.

In 2010 GMV became the main contractor for the design, maintenance, deployment and evolution of the Eurosur network for the Frontex Agency. The collaboration began with a pilot project and then moved onto a fully-fledged framework contract between the multinational and the Agency.

For the European External Actions Service (EEAS), moreover, GMV is priming the design and development

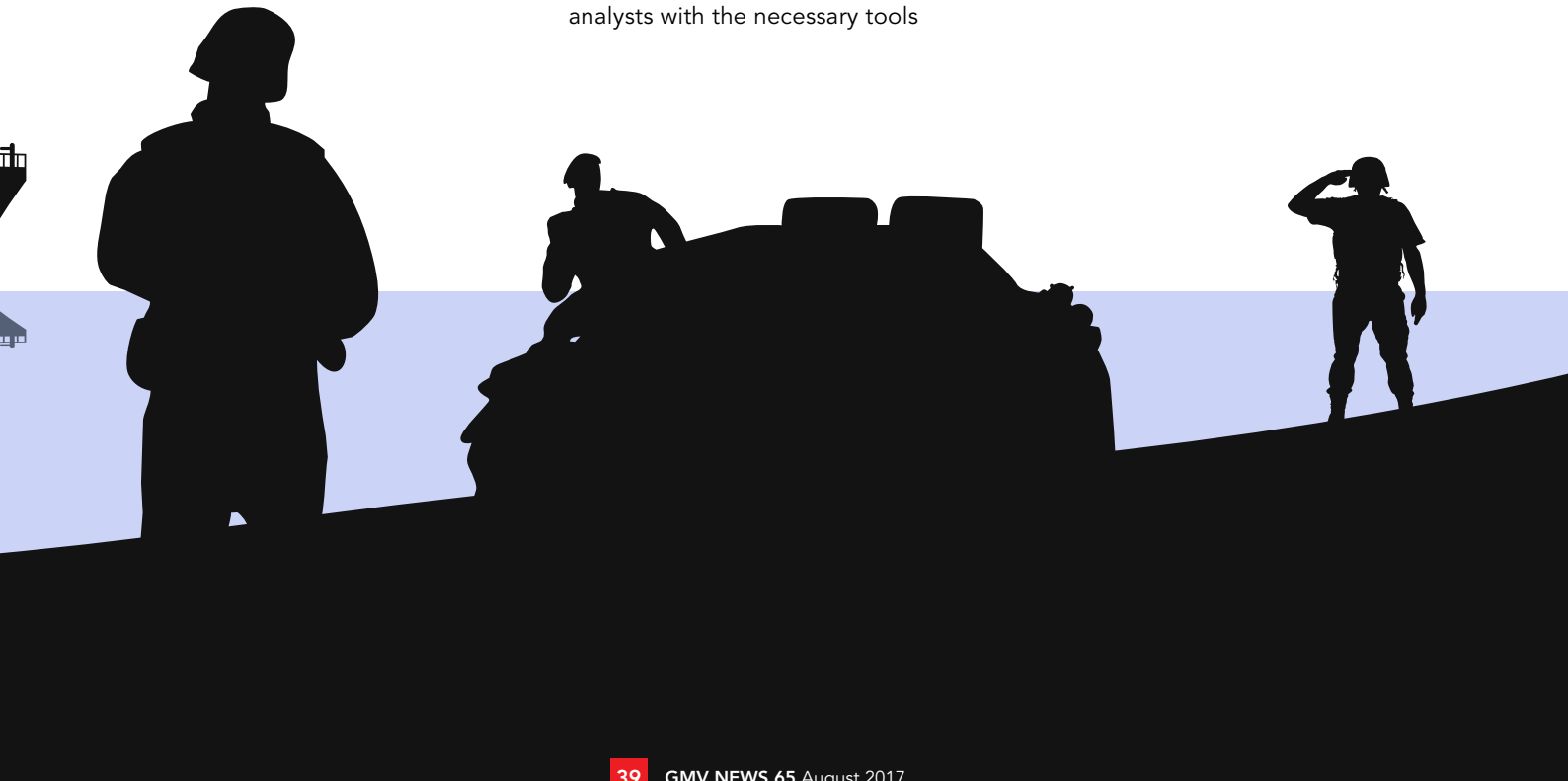
of the European Command and Control Information System (EUCCIS) used by EEAS on its missions outside Europe.

GMV is also a longstanding collaborator of the European Maritime Safety Agency (EMSA) in such activities as studies to pinpoint the user benefits of Remotely Piloted Aircraft Systems (RPAS) in the marine environment or the provision of ICT services. In the area of satellite image processing and remote sensing, GMV is priming a framework contract for SatCen.

In the JISR area (Joint, Intelligence, Surveillance and Reconnaissance), and as part of Spain's participation in NATO's MAJIIC project, GMV is collaborating with diverse NATO organizations as well as MoDs of NATO member countries on both sides of the Atlantic, offering its inhouse Mobile ISTAR Exploitation system (called SEISMO after its Spanish initials: Sistema de Explotación ISTAR Móvil), CSD (Coalition Shared Database), Atenea (IRM&CM Tool) and COLLECTOR (ISR sensor simulator), which pools information from many different sources to provide intelligence analysts with the necessary tools for exchanging ISR information and performing workflows that enable interaction throughout all JISR phases.

GMV also features large in European Commission security-research framework programs, especially H2020 and its forerunner FP7. The multinational's activity centers on the maritime surveillance area by participating in diverse projects such as CLOSEYE (Collaborative evaLuation Of border Surveillance technologies in maritime Environment bY pre-operational validation of innovativE solutions), EUCISE2020 and MARISA (Maritime Integrated Surveillance Awareness).

These activities have all helped to raise GMV's worldwide security-and-defense profile, winning the company pole position in this sector. Levering Europe's current drive towards a common security and defense policy, the company's medium-term plans include consolidating its current strong international position and ensuring its sustained growth into the future.



Another step towards operational deployment of SAPIIEM systems

AS PART OF GMV'S SUPPORT ACTIVITIES TOWARDS OPERATIONAL DEPLOYMENT OF JISR (JOINT INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE) CAPABILITY, THE COMPANY HAS SUPPORTED THE SPANISH ARMED FORCES' PARTICIPATION IN DIVERSE NATIONAL AND MULTINATIONAL EXERCISES

The JISR activities are carried out by means of the SAPIIEM systems (ATENEA, SEISMO, CSD, SIERRA Tools, C2NEC, COLLECTOR) developed by GMV under its contract with the Directorate General of Armaments and Material (Dirección General de Armamento y Material: DGAM) of the Spanish MoD. These systems have now demonstrated a high degree of interoperability in multinational exercises, ensuring proper exchange of information with similar systems furnished by NATO and other countries.

During the first half of 2017 the Spanish armed forces made use of these systems within diverse exercises. The most noteworthy were the following: the national MOPEX exercise to evaluate the performance of operations command (MOPS in Spanish initials) in planning and running a joint operation; the NATO STEADFAST COBALT 17 (SFCT17) exercise to trial and validate C4ISR interoperability in support of the NATO Response Forces (NRF) for 2018, and in particular where the special operations joint command (MCOE in Spanish initials) is evaluated as NATO NRF18 command; and lastly in the SOCCEX exercise for national preparation of the MCOE for NATO operational evaluation visits to be held in late 2017.

Employment of SAPIIEM systems in all these exercises, with GMV support, has helped to guarantee successful performance of JISR activities as one more step towards operational deployment of these systems.

The FORTRESS security project appraised as a success by the European Union

The FORTRESS (Foresight Tools for Responding to cascading effects in a crisis) project has recently been brought to a close. The aim of this three-year, European-Commission-funded project was to ascertain the cross-border, cascading effects of crisis situations in different contexts of interconnected infrastructure.

The project's overall purpose was to ensure crisis response capability, steering between the twin reefs of, on the one hand, an over- reliance on unstructured information collection and, on the other, a lack of attention to structural communication and management elements of cross-border, cascading crisis situations. To do so it has used state-of-the-art information-collection and modelling tools to assist stakeholders in gauging what information is significant, relevant and of greatest priority so they can adjust their actions accordingly.

Within the project, carried out by thirteen partners from eight European countries, GMV led development of the FORTRESS Incident Evolution Tool (FIET), a user-friendly tool that calculates infrastructure, systems and geographical areas affected by an emergency even between different organizations and or countries. FIET can be used as a decision-support foresight tool to assist decision-makers in understanding the potential effects of their actions in training environments.

These three years of work have managed to pinpoint potential effects and generate game-changing concepts, measuring criteria and strategies for a better inter-sector management of crises. The project received an excellent appraisal in the European Commission's final review, in which FORTRESS was hailed as a complete and exemplary success story.

First deployment of the EU's Command and Control Information System

SUCCESSFUL COMPLETION OF THIS DEPLOYMENT REPRESENTS THE FIRST STEP TOWARDS A LONG-TERM COOPERATION FRAMEWORK AS A TRIED-AND-TRUSTED SUPPLIER OF EEAS (EUROPEAN EXTERNAL ACTION SERVICE)

Within the framework contract of the European External Action Service (EEAS) for maintenance, support and evolution of the EU's Command and Control Information System, in which GMV is acting as sole contractor, new software has recently been deployed for implementation of the upgrades shown to be necessary during the first year of execution.

The European Union's Command and Control Information System (EUCCIS) is used by EEAS on its missions outside Europe for planning, monitoring and conducting EU-coordinated crisis management operations.

The upgrades phased in during this first year of execution have focused on bringing the system more closely into line with user needs, especially the work carried out in the collaborative portal for exchanging information between the command posts deployed in the theater of operations and the Brussels operation center. This has involved a revamping of the portal to achieve the paradigm change requested by users, in the interests of adapting the portal seamlessly to the various stakeholder communities (enabling collaboration between both civil and military groups) and achieving better segmentation of the contents of particular interest to each one.

The new components were deployed in a production environment in April, while the Site Acceptance Tests (SATs) were conducted by operational users in May.

The European External Action Service has expressed its satisfaction with GMV's work. Successful deployment and testing of the system proved possible using up far fewer resources and time than before GMV's participation in the scheme. End users, moreover, have confirmed improvements in the new system. Worthy of mention also is that the test-driven approach of this development cut down the number of testing incidents to a bare minimum.

Successful deployment and testing of the system proved possible using up far fewer resources and time than before GMV's participation in the scheme

GMV at Portugal´s latest NATO Conference

Cyberspace has no physical borders; cyber threats are now acquiring increasing disruptive and destructive power. In light of these two crucial factors NATO's strategic vision highlighted the need of setting-up a cooperative cyber defense capability in order to meet current and future security and defense challenges. According to the NATO Strategic Concept, adopted in November 2010 in Lisbon, the Smart Defense concept seeks to stimulate synergies and foster Allied Nations' cooperative efforts, in order to ensure development, acquisition and maintenance of the necessary military capabilities.

Smart Defense is thus assumed by NATO as a way of ensuring non-duplication and integration of national capability development initiatives (pooling and sharing), in the interests of better prioritization and coordination of efforts between NATO and Allied Nations. In the cyber defense area, there are already three Smart Defense Projects: Multinational Cyber Defence Capability Development (MN CD2), Malware Information Sharing Platform (MISP) and Multinational Cyber Defence Education and Training (MNCDE&T). NATO's Smart Defense calls for a renewed cooperation culture and requires an innovative approach in order to enhance the Alliance's Cyberdefense.

In the 3rd NATO Cyber Defence Smart Defence Projects Conference (CD SDP), held at the Military Academy of Amadora at the end of April, special attention was given to NATO's cooperation with Industry and Academia and to new NATO-EU cooperation opportunities in the cyber field. In line with this idea, NATOS´s Cyber defense-related Projects (MNCD2, MISP and MNCDE&T) all have the overriding remit of joining forces and working together with industry and academia, building the necessary bridges between international and national initiatives.

GMV, with proven experience in the Cybersecurity sector, took part in the Conference to show how the latest Cybersecurity and Cyber defence technological breakthroughs might help to meet the current challenges faced by the different state security corps and forces.

José Neves, Security and Defense Director of GMV Portugal, was on hand to attend the main security corps and forces representatives, such as the Portuguese Secretary of State for Defense and the Chief of the Portuguese Armed Forces. Representatives from several countries (Spain, USA, Brazil, Algeria, etc.) and international organizations (namely the European Defence Agency and NATO) also took the chance to visit GMV's stand and gain a more thorough understanding of the company's strategy for this market.

GMV helps to improve Europe's maritime surveillance

The Common Information Sharing Environment (CISE) is a European-Commission-brokered maritime-surveillance initiative that establishes a collaborative process between European authorities to improve maritime situational awareness.

The Commission has been developing the CISE concept since 2009 in collaboration with military and civil authorities of member countries. A legal, political and organizational framework has been defined to allow the exchange of information among stakeholder sectors (defense, state security forces and corps, maritime rescue service, customs authorities, border control authorities, fishery and the environment).

As part of the work for defining this concept it is necessary to define a series of systems, networks and services that have to be integrated in a comprehensive information infrastructure to ensure CISE operability by 2020.

The Commission has therefore launched an FP7 operational validation project called EUCISE2020. This project comprises 37 partners from 15 different countries, including the Spanish MoD through the navy and other Spanish institutions like the Guardia Civil, the Maritime Rescue Service (*Salvamento Marítimo*) and the taxation authority (*Agencia Tributaria*).

Within this project the industry has been invited to submit R&D bids for the creation of information-exchanging EUCISE nodes. These nodes follow a service-based architecture defined using the NATO Architecture Framework (NAF) and employing technical standards to guarantee interoperability between nodes. GMV is playing a key part in this project on the strength of its interoperability experience and expertise in both civil and military projects.

This approach clearly chimes in with the Spanish MoD's Global ICT System Architecture (*Arquitectura Global de Sistemas de Tecnologías de la Información y Comunicaciones*) as recorded in the Secretary of State for the Defense's Instruction 58 of 28 October 2016.

This solution will be deployed in civil and military institutions of several EU countries, with Spanish nodes being set up in the navy and Guardia Civil. These nodes will be validated in operational use during a six-month period running from November 2017.

MARISA: Merger of Data and Big Data for Maritime Traffic

An operator clocks on in the Regional Center for Maritime Vigilance of the Mediterranean. During this operator's shift an alert is tripped on the screen. A merchant ship has ceased to emit AIS. Satellite data shows the ship is still there, following the same heading as in previous hours. This does not tally with its declared destination port. The ship has switched flags en route, something it usually does at this time of year, but when heading for another port. The software also detects unusual social-media activity by the merchant ship's crew, trying to sign up with other ships or taking selfies for other networks with comments that smack of farewells. The ship's log, however, shows no signs of any previous undeclared cargo. After weighing up all the information, the operator decides to pass on the alert to the boss, who then orders action to be taken against the merchant ship's suspicious activity.

Meanwhile, another operator, this time in the North Sea, is using the software to assess the state of a recreational vessel caught up in one of the frequent harsh storms in this sea. The time has come to coordinate rescue activities.

Members of the MARISA project. Laurea University of Applied Sciences (Helsinki)

Such scenarios could be possible in the near future thanks to the EU-funded, H2020 MARISA (Maritime Surveillance Awareness) project. MARISA brings together 22 organizations, including national and multinational firms from each participating country, national and NATO research institutes and end users (military navies, coastguards and the Spanish Guardia Civil).

GMV, playing a key role in the project, holds responsibility for system design, the development of several data-fusion and anomaly-detecting algorithms, as well as the Iberian trial to be held in collaboration with the Spanish Guardia Civil and the Portuguese Marinha.

The main driving forces behind this project, officially initiated in May, are innovation and border-surveillance development of Big Data and Multisensor data-fusion technology, together with satisfaction of end users' operational needs.

Conference on the "Global architecture of the Ministry of Defense for a national standardization and interoperability model"

In November of last year the Secretary of State for Defense published Instruction 58 of 28 October 2016 approving the Global Architecture of ICT Systems of the Ministry of Defense. This benchmark architecture sets out a series of principles for developing systems for the ministry.

On 29 November, to bring this milestone event to wider notice, the ICT Systems Center (*Centro de Sistemas y Tecnologías de la Información y las Comunicaciones*: CESTIC), together with the Defense and Security Technology Foundation (*Fundación Círculo de Tecnologías para la Defensa y la Seguridad*) organized a conference on the "Global architecture of the Ministry of Defense for a national standardization and interoperability model".

Inaugurated by Agustín Conde Bajén, Secretary of State for Defense, the conference included a panel discussion involving GMV together with other representatives of defense companies.

In this panel discussion Héctor Naranjo Setién stressed that "*this architecture will turn out to be highly beneficial for efficient, hi-tech companies like GMV, boosting their chances of winning tenders on the strength of high-quality bids thanks to the capacity of reusing components and technologies and a clearer definition of the work to be carried out*". "*GMV boasts a wealth of experience in all these methodologies, standards and technologies, using them all extensively in various national and international projects.*"

GMV in Europe's Cybersecurity shop-window

infosecurity EUROPE

Cybersecurity is nowadays considered to be a top-priority matter by the European Commission. Not only does it feature as one of the pillars of the EU's R&D framework programs but it has also been systematically taken up by community and member-state politicians.

And the truth is that Cybersecurity is now a critical factor in guaranteeing Europe's digital transformation, a sine qua non of technological progress. Unless Europe manages to build up a strong Cybersecurity sector with its own technology we are bound to be exposed to increasingly complex and impactful cyberattacks.

Infosecurity Europe 2017 has now been held with the aim of bringing together experts and sharing information on the latest technological breakthroughs for combating the threats currently hovering over organizations all over the world. This event, considered to be number one in Europe, turned London into the epicenter of international security. No Cybersecurity professional could afford not to be there, so a sector-benchmark firm like GMV could hardly miss it either.

GMV's experts displayed the company's eyecatching range of Cybersecurity products and services, such as ***gestvul***, ***checker ATM Security***, ***atalaya*** and ***arkano***. It also unveiled other solutions like ***FARO Security***, a platform that represents a huge stride forward in today's company security management.

The event attracted 240 speakers, 360 exhibitors, and a total turnout of about 18,000. GMV's solutions shared the stage on an equal footing with the other most advanced technology on today's Cybersecurity market.

GMV collaborates with CCI to tackle Industrial Security

THE BEST WAY OF PROTECTING ANY INDUSTRIAL PLANT'S DIGITAL TECHNOLOGY IS ACKNOWLEDGING THE IMPORTANCE OF CYBERSECURITY AND MAKING A FIRM COMMITMENT TO IT FROM THE VERY FIRST STAGES OF THE WHOLE LIFECYCLE

Industry is being hit by just the same threats and vulnerabilities as the IT world. Pundits argue that the best way of protecting any industrial plant's digital technology is acknowledging the importance of Cybersecurity and making a firm commitment to it from the very first stages of the whole lifecycle. This means phasing in checks and measures to meet cyber-protection needs and ensure the proper working of any industrial process as well as protecting the very process itself, doing so during all production stages (design, supply, installation and commissioning).

Spain's Industrial Cybersecurity Center (Centro de Ciberseguridad Industrial: CCI), with the special participation of Técnicas Reunidas, has just published the document "Cybersecurity in an Industrial Automation Project Lifecycle". This guide aims to contribute towards the crucial task of improving the protection of automated industrial infrastructure. GMV's Javier Zubieta, Cybersecurity Business Development Manager of GMV Secure e-Solutions, has input his expertise and experience to help draw up the contents.

The growing development of Industry 4.0-enabling technologies opens up more attack vectors, which now need to be tackled to ensure safe operation.

"This publication will help to fill the legal loophole of Cybersecurity management in industrial control and automation systems" **points out Javier Zubieta**

Towards intelligence in Cybersecurity

"WE NEED TO GO FURTHER, FOLLOWING A PROACTIVE AND REACTIVE STRATEGY, PREEMPTING THREATS AND RESPONDING TO THEM QUICKLY WHEN THEY DO OCCUR" JOSÉ MARÍA LEGIDO, NORTHEAST REGION MANAGER OF GMV SECURE E-SOLUTIONS

At the beginning of this year IDC forecast that over 70% of corporations will suffer a massive cyberattack by 2019. Sad confirmation of this prediction came a few months later with May's slew of worldwide ransomware attacks, infecting thousands of information systems in scores of countries. Taking his cue from this, José María Legido, Northeast Region Manager of GMV Secure e-Solutions, gave a speech at the Predictions Barcelona conference, organized by IDC and IDG, stressing the vital importance of working with a technology-and business-risk management system, as well as a security architecture, informed and aware personnel, threat response and law abidance (especially with the new GDPR coming into force in 2018).

Legido highlighted the lack of security and the difficulty of identifying the hackers. "*We need to go further, following a proactive and reactive strategy, preempting threats and responding to them quickly when they do occur*", he argued. An awareness of the problem is crucial and also of the risk posed by the constantly growing threat to companies, public organizations, services, people, critical infrastructure and new paradigms such as quantum computing.

Might we get to see unknown threats? GMV proposes working towards intelligence of SIEM (Security Information and Event Management), making the eyes and ears of our IT platform intelligent. "*There is a possibility of aggregating events of an organization's various SIEMs, tagging on new external or internal information sources and feeding SIEM with new intelligent rules such as Big Data and Machine Learning*" added Legido. The aim in view is to process and analyze vast amounts of information, establishing the etiology and studying complex behavior with great predictive capacities and advanced analytical skills way beyond the possibilities offered by today's traditional SIEMs.

José María Legido argued that the new generation of threats now looming up and improving security to suit will call for increasingly intelligent systems capable of proactively detecting threats and acting accordingly to forestall or mitigate their impact.

GMV reinforces its Cybersecurity leadership with Imperva

GMV has become the first ever firm in Southern Europe to be named by Imperva as a Platinum Partner. This designation is the culmination of a seven-year collaboration between both organizations, helping customers to deploy data-protecting Cybersecurity solutions and ensure regulatory compliance.

"GMV is a committed partner, and we're delighted that they're being recognized for their excellent Cybersecurity work and outlay" said Bertrand de Labrouhe, Area Vice President Southern EMEA & Mediterranean at Imperva

"This recognition as an Imperva Platinum Partner sets our company apart, strengthens our Cybersecurity leadership, and enables us to offer our clients the most innovative application- and data-protection solutions" says Javier Zubieta, Cybersecurity Business Development Manager at GMV Secure e-Solutions.

To become an Imperva Platinum Partner companies must exhibit proven success in implementing and supporting the Imperva Cybersecurity portfolio, which includes the product lines Imperva Camouflage, CounterBreach, Incapsula and SecureSphere; they must also have great security expertise and furnish their staff with Imperva-certified technical resources.

"GMV is a committed partner, and we're delighted that they're being recognized for their excellent Cybersecurity work and outlay," said Bertrand de Labrouhe, Area Vice President Southern EMEA & Mediterranean at Imperva. *"GMV and Imperva will work together to help enterprises in Spain protect their business-critical data and applications both on-premises and in the cloud and to prepare for the upcoming General Data Protection Regulation (GDPR), to be enforced as from May 2018."*

EAST FCS Forum brings together the world's ATM-protection experts

GMV TOOK PART AS SPONSOR WHILE ITS ***checker ATM Security*** TEAM SHOWCASED THE WORLD'S FIRST SOFTWARE SPECIFICALLY DESIGNED FOR ATM FRAUD PROTECTION. WITH TEN YEARS' EXPERIENCE BEHIND IT, ***checker ATM Security*** IS NOW THE WORLD'S LEADING ATM PROTECTION SOLUTION, WITH OVER 120,000 LICENSED SYSTEMS INSTALLED IN OVER 40 DIFFERENT BANKS

Logical attacks on ATMs are on the increase throughout Europe and in many other parts of the world too. In its 2016 report, EAST (European Association for Secure Transactions) reported that cyberthreats in this sector had hit an all-time high in 2016. Up to now cybercriminals' attacks had been based on ATM-related malware, cloned credit cards and bank Trojans. In recent years, however, attacks have diversified, raising further qualms about this problem around the world. To perpetrate their attacks now the hackers are trying to break into the networks of financial institutions and initiate their attack from inside. On the other side of the battlefield, Cybersecurity expert are developing solutions to forestall these new threats.

EAST FCS Forum 2017 is an event aimed at professionals involved in identifying, preventing and detecting security risks and ATM-related crime. Held in the Hague, the Netherlands, the forum assembled worldwide experts to swap information on the latest threats and the financial sector's countermeasures. Attendees were also given practical information about what organizations are now doing to combat these risks.

Self-Service Banking Asia 2017

GMV and the Malaysian Electronic Payment System (MEPS) have come together on the same stage to explain the new malware threats and the groundbreaking solutions continually being developed and upgraded by technology companies to head them off. The stage in question was "Self-Service Banking Asia 2017", organized by RBR (Retail Banking Research) and reckoned to be South East Asia's leading ATM protection conference. This area is one of the world's quickest growing regions in terms of banking Cybersecurity solutions.

Carlos Sahuquillo, Security Consultant of GMV Secure e-Solutions shared his expertise on this matter, giving a paper under the title "ATM Logical Security: adapting to new threats". Together with Marcus Lim Wooi Loon, Head of the Self-Service Terminal Business and Operations Division in MEPS (Malaysian Electronic Payment System), he also explained how this financial association has enhanced its ATM security with GMV's help.

The GMV expert's speech stressed the need of an ATM-Cybersecurity paradigm switch: "*today's reactive response has to change. We're always one step behind. We now have to think like a hacker and act proactively to head off any threats*".

IDESCAT ensures compliance with Spain's security legislation

THE CATALAN STATISTICS INSTITUTE (*INSTITUTO DE ESTADÍSTICA DE CATALUÑA*: IDESCAT) HAS ONCE MORE TURNED TO GMV TO ENSURE ITS ONGOING COMPLIANCE WITH SPAIN'S NATIONAL SECURITY SCHEME (ESQUEMA NACIONAL DE SEGURIDAD: ENS) AND PERSONAL DATA PROTECTION LAW (*LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL*: LOPD)

For this purpose GMV ran an audit to pinpoint any nonconformities or improvable shortfalls. It also worked on an improvement of organizational aspects to guarantee ENS- and LOPD-compliance, plus a check of all security-improvement actions taken after the company's 2014 audit.

As a result of the examination of all the Institute's information systems and files (computerized or otherwise) as well as physical security or enforcement legislation, GMV drew up an action plan focusing in particular on amendments published by the ENS on 4 November 2015. Since GMV's first IDESCAT audit back in 2011 there has been constant improvement and upgrading of ENS- and LOPD-compliance as well as the overall state of security.

The ENS lays down the security policy for the use of electronic media. It is made up by basic principles and minimum requisites to ensure proper protection of information. The overall aim is to guarantee trustworthiness of electronic media in the eyes of citizens. The purpose of the LOPD, for its part, is to guarantee and protect personal data processing activities, public freedoms and the fundamental rights of individuals, especially their honor, personal and family privacy and intimacy.

GMV innovation in European healthcare research projects

"LIVING LONGER AND BETTER" IS ONE OF OUR SOCIETY'S RIGHTFUL GOALS. TWO OF THE SUREST MEANS TOWARDS THIS END, TO THE BENEFIT OF ALL CITIZENS, ARE INNOVATION AND PUBLIC-PRIVATE COLLABORATION

Living longer and better is one of today's society's rightful demands and is also the working goal of many researchers, physicians and engineers, healthcare professionals in the public and private sector. Two of the surest means towards this end, to the benefit of all citizens, are innovation and public-private collaboration. And all this needs to be done on the strength of personalized, patient-centered healthcare that is sustainable over time.

European Research Programs are pursuing the same goal, funding projects such as FACET, HARMONY, MOPEAD and PAPHOS, in all of which GMV is inputting its hi-tech expertise. These projects call for a huge coordination effort, involving as they do many members of varying types from different countries.

Harmony, in particular, involves fifty one European partners with GMV as the sole technology firm; this consortium is carrying out cutting-edge research to improve and personalize the treatment of patients with chronic lymphocytic leukemia, non-Hodgkin lymphoma, myelodysplastic syndromes and blood disorders in babies and children. GMV's particular input to the project is the design and development of the Big Data platform for mass processing of information to help physicians in their decision-making procedures.

In the MOPEAD project for clinical-scientific research into Alzheimer's disease, GMV is developing a web app based on the Citizen Science concept for recruitment of early-phase Alzheimer patients. It is also deploying and implementing a Big Data system for analysis of the data recorded from these patients.

Preventive care and wellbeing are becoming increasingly important nowadays, while diagnosis procedures and the management of illnesses

are acquiring a higher degree of certainty. In this overall context, GMV's particular aim in the PAPHOS project is to create a secure platform applying cutting-edge analytical technology to allow all healthcare stakeholders to move on from the reporting phase (what happened?) to the predictive phase (what might happen?) and the prescriptive phase (why will it happen?).

Although pundits tell us that the human species has lengthened its life expectancy by thirty years, the challenge now lies in improving the quality of this additional time. With this aim in mind the EU is now driving the FACET project, in which GMV's inhouse telemedicine platform ***antari HomeCare™*** is helping elderly people in a state of special vulnerability and high disability risk. This platform can care for them, monitor them and watch out for chronic illnesses, storing and managing their healthcare data as well as planning and monitoring their treatment.

GMV is inputting its hi-tech expertise in FACET, HARMONY, MOPEAD o PAPHOS projects

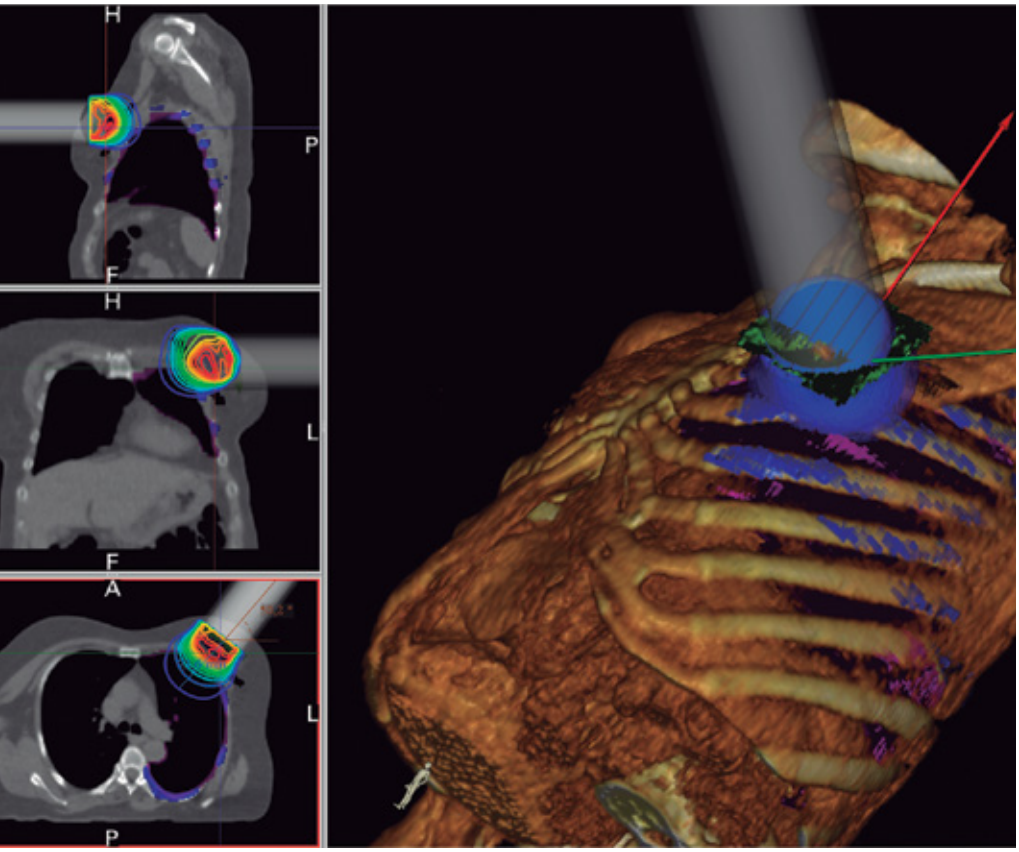
GMV technology at the service of the European RAINBOW project

GMV'S INPUT TO THE ONGOING QUEST FOR MORE PERSONALIZED MEDICINE RESTS ON ITS WEALTH OF EXPERIENCE IN DEVELOPING SUCCESSFUL CLINICAL SIMULATORS SUCH AS THE SURGICAL SIMULATOR INSIGHT AND THE INTRAOPERATIVE RADIOTHERAPY PLANNER ***radiance***

GMV is now working on the development of the next generation of practical, user-friendly biomechanical simulation systems that optimize the design of personalized clinical treatment. So user-friendly are these machines that clinicians can handle them without technicians' help. This project falls under the umbrella RAINBOW project, included in the Innovative Training Networks (ITN) of the Horizon 2020 program.

The aim of the project "Rapid biomechanical simulation for personalized clinical design" (RAINBOW) is to build up knowledge in specific areas of clinical simulation. This will involve a threefold approach: firstly, innovation and research, secondly, collaboration with industry to gauge the clinical impact of developments and thirdly training and instruction. During the four-year project GMV will be collaborating with the other participating research organizations, including Cardiff University in Wales Universidad Rey Juan Carlos in Spain , Luxembourg University, Aalborg and Kobenhavns Universities in Germany, France's National Scientific Research Center and Hvidovre Hospital, among others.

GMV's input to the ongoing quest for more personalized medicine rests on its wealth of experience in developing successful clinical simulators such as the surgical simulator ***insight*** and the intraoperative radiotherapy planner ***radiance***.



BENEFITS OF THE PROJECT

The physiological, anatomical and biomechanical simulation skills built up by the RAINBOW project researchers will stand them in good stead for developing next-generation computational clinical modeling solutions.

GMV boasts a long and distinguished track record of developing ICT-based healthcare innovation and this now underlines its ongoing drive to develop production-quality rapid biomechanical simulation technology and train up highly-skilled personnel to use it.

In the words of Carlos Illana, product manager for GMV's inhouse radiance planner, the RAINBOW project, pursuing the overall aim of the Innovative Training Networks *"will contribute towards the training of a new generation of creative and game-changing researchers capable of pushing back the envelope, to the economic and social benefit of the whole European Union"*. In this particular case these breakthroughs will come in the development of clinical simulation tools to be applied in diagnosis, prognosis, monitoring, surgical training, planning, guidance, prosthesis design, implant operations and medical devices.

GMV's e-Health platform at the service of the Colombian Campbell Clinic and the Ópticas 2000 opticians chain

The Colombian Grupo Campbell clinic, a leading specialist in the treatment of traffic-accident victims, has taken up GMV's ***antari*** e-Health system for the diagnosis, prescription and monitoring of its patients, greatly speeding up healthcare procedures in these situations.

The versatility of this inhouse telemedicine platform, with specific developments for telepediatrics and ophthalmology, has also caught the eye of a new leading opticians chain, Ópticas 2000, a company of the Spanish distribution group, El Corte Inglés. Ópticas 2000 has taken up ***antari*** for providing remote ophthalmology services, now available on client demand in all its opticians outlets.

GMV's *antari* e-Health system for the diagnosis, prescription and monitoring of its patients, greatly speeding up healthcare procedures in these situations

The GMV-developed tele-ophthalmology platform, providing the service by video conference in real time, enables clients of the El Corte Inglés opticians chain to receive on-the-spot specialist diagnosis without needing to visit the dispensing ophthalmologist. The firm is thus able to add value to the service provided for its customers, saving them long journeys to visit the specialist and making the whole procedure of acquiring glasses or contact lenses much more trustworthy.

GMV shares its experience of public healthcare procurement

Carlos Royo,GMV's Healthcare Business Development Manager

In the event "Food- and Healthcare-Company Collaboration in the ICT Sector" (*Colaboración empresarial en el sector TIC aplicadas a la salud y la alimentación*) the Regional Authority of Castilla y León (*Junta de Castilla y León*) has presented its game-changing public procurement initiative for modernizing the region's health and social care for chronic patients and people living in a situation of dependence. Carlos Royo, GMV's Healthcare Business Development Manager, talked about one of the company's inhouse healthcare ideas towards this end.

GMV's antari platform for monitoring chronic patients with multiple illnesses makes the company a solid ally in this project driven by the Social Services Office (*Gerencia de Servicios Sociales*), the Regional Health Office (*Gerencia Regional de Salud*) and the Entrepreneurial Innovation, Financing and Internationalization Agency (*Agencia de Innovación, Financiación e Internacionalización Empresarial*) of Castilla y León to facilitate monitoring of chronic patients and people living in a state of dependence.

This event was jointly organized by the Platform of Technologies for Health and an Active and Independent Life (*Plataforma de Tecnologías para la Salud y la Vida Activa e Independiente: eVIA*) and FoodForLife, with the collaboration of the Entrepreneurial Innovation, Financing and Internationalization Agency (*Agencia de Innovación, Financiación e Internacionalización Empresarial*) of the Junta de Castilla y León and the Technical Directorate of Planning and Access to Social Services (*Dirección Técnica de Ordenación y Acceso a los Servicios Sociales*) of the Gerencia de Servicios Sociales.

GMV grafts improvements onto Cyprus's public-transport modernization project

The Public Works Department of Cyprus's Ministry of Transport, Communications and Public Works has once more placed its trust in GMV for upgrading the government's nationwide public bus fleet modernization project.

This contract extension includes installation of 60 onboard video recording units, to be managed by GMV's onboard REC30 unit, which combines in a single device the tracking equipment, fleet-management equipment and CCTV video recorder with online streaming. This system is already successfully up and running in all buses of the island of Malta as well as other projects carried out in Spain, Poland and Malaysia.

Apart from the onboard IP video cameras, this equipment will also connect up to TFTs to give onboard visual information as well as ridership counters.

The project also takes in a contactless farecard recharging website using Desfire EV2 technology. For this purpose GMV's system will plug into a JCC banking payment platform, which is the most widespread throughout the country. Future phase-ins will then allow this bus farecard to be used later for other government services.

The project also includes adaptation of a series of vehicles to receive GMV's onboard equipment. These vehicles, mainly vans adapted for public transport purposes, lack the classic onboard fastening devices, so GMV has had to rethink these vehicles completely to come up with a personalized solution for each model.

GMV presents its whole range of public-transport products and services at Montreal's UITP Summit 2017

GMV was present at the 62nd Global Public Transport Summit of the International Association of Public Transport (UITP) hold from 15 to 17 May, 2017, in Montréal.

UITP is the international organization that brings together the world's main public-transport stakeholders, acting as a worldwide contact network for exchanging ideas on the best practices in this area. This Brussels-based association, born in 1885 with 63 members, has by now built up this membership to a total of 1400 companies.

GMV presented its whole range of solutions for the Public Transport such as its fleet management systems for urban and interurban transport, passenger information systems and electronic fare collection systems. Several demos of GMV's advanced ITS for Public Transport were hold at GMV stand.

GMV's experts in Public Transport Technologies also participated in the exciting focus sessions which took part altogether with the exhibition. Particularly, the Focus Session Planning: System, Trip and Mobile Apps included a presentation of ***gmv planner*** powered by DPK, the latest product in GMV's ITS portfolio.

gmv planner is a comprehensive Planning & Scheduling platform which provides the Public Transport Authorities and Operators with a powerful Public Transport Operation Lifecycle Management tool.

GMV's stand also included a corner for GMV's North American subsidiary, Syncromatics, which run demos and presentations of our SaaS Fleet Management system customized for the US market.

First takeup of the optimum planning system, *gmv planner*

GMV HAS BEEN CONTRACTED BY THE MAJORCAN PASSENGER-TRANSPORT COMPANY TRANSABUS DE TRANSPORTE COLECTIVO DE VIAJEROS DE MALLORCA FOR SUPPLYING ***gmv planner***, AN APPLICATION SPECIALLY DESIGNED FOR TRANSPORT COMPANIES' SERVICE PLANNING

This contract represents GMV's first ever client reference in Spain for systems of this type, with which it now completes its range of ITS products and services. This new system manages the whole transport cycle, from initial configuration of lines and schedules, service planning and operational control to the final passenger-information systems.

gmv planner powered by DPK is a comprehensive planning and scheduling platform that provides public transport authorities and operators with a powerful public transport operation lifecycle management tool. It solves all service planning and scheduling problems, breaking them down into working timetables for vehicles and drivers to suit existing business rules and constraints. It also cuts down running costs and increases the number of services on offer. The initial outlay is recouped in a very short time and it also avoids many time-consuming tasks, working quickly and efficiently with a significant amount of data in an integrated way (work-schedule planning time alone is cut by a factor of 20).

gmv planner allows Transabus to manage the complete service lifecycle in a continuous dataflow on the basis of integrated modules catering for activities with varying timeframes and frequency:

- Long-term service planning (driver holidays, transport network, schedules, services); mid-term (rostering); and short term (adjustments of assignments and scheduling).
- On-service operation support (vehicle-dispatching and daily control).
- Analysis of the service provision afterwards and harnessing of this information in corporate systems (payrolls, Corporate ERPs / SAPs, etc…)
- Planning of the maintenance of each vehicle after service evaluation.

gmv planner has been successfully set up in road- and railway-transport operators in Europe and Asia and is now being used for planning the service of thousands of vehicles

GMV upgrades Szczecin's public transport system

AS PART OF ITS LONG-TERM RELATION WITH ZDITM SZCZECIN (SZCZECIN TRANSPORT AUTHORITY) GMV HAS WON THE CONTRACT FOR GRAFTING NEW FUNCTIONS ONTO THE SYSTEM ORIGINALLY ROLLED OUT BACK IN 2015

ZDITM Szczecin has been GMV's customer since 2010, with the signing of a contract for implementation of the first phase of an advanced fleet management system complete with passenger information system, real-time CCTV plus electronic fare-collection system. Since then both companies have been liaising and cooperating nonstop to make the transport service and system even more passenger-friendly.

This new contract phases in improvements to the passenger-information-system and fare-collection-system reporting tool. One of the most important changes for the customer comes in the area of passenger information. A new function allows static passenger information to be removed from street displays and the web page if the vehicle concerned was prevented from completing the run by technical problems. This will ensure swifter passenger information about all changes in the transport services.

Furthermore, there will be a new configuration for vehicles and for busstop- and station-displays. As a result passengers will now know if the arriving vehicle offers the possibility of buying the ticket in the onboard ticket-vending machine. Information will be shown in displays next to the line destination, with pictograms indicating the possible on-vehicle fare-payment methods (bank cards, cash and ePurse).

These new functions will allow ZDITM Szczecin to adapt the system to their current requirements and furnish passengers with top-quality trip-planning information.

GMV phases new functions into Bydgoszcz's Intelligent Transportation System

GMV has signed a contract with Bydgoszcz Transport Authority, ZDMiKP, for an additional year of ITS maintenance. This new agreement covers all technical customer support plus maintenance of the equipment installed in the 287 vehicles and 35 passenger information displays. GMV is also responsible for delivering new server infrastructure, developing new system functions and adapting them to suit the customer's current needs.

These new functions include modifications of the street-display content manager application plus an ITS topology creation and configuration app (Edition SAE). Changes will be also made in reports used by the Transport Authority for settlements with transport operating companies.

One of the most important new functions for the customer is Edition SAE's application for defining a temporary topology version. This modification makes it possible to dump current temporary topology to one of the backups and to load one of the backups to temporary topology. This new function means it is now possible to work with a historical topology without forfeiting the current one, doing so by copying current topology to one of the backup topologies and then recovering the historical one. Once the work with the historical topology has finished, the user will be able to load the previous topology back onto the system.

Cooperation between GMV and Bydgoszcz Transport Authority dates back to 2011, when GMV won a contract for setting up an advanced fleet-management system and control center for its whole fleet. Since that time, GMV has been providing all ZDMiKP services, winning excellent passenger feedback.

GMV forges even closer relations with Alstom

ON 4 MAY ALSTOM'S HEAD OFFICE IN PARIS HOSTED THE AGREEMENT WHEREBY GMV JOINED THE ALSTOM ALLIANCE CHARTER, ALSTOM'S STRATEGIC PROGRAM FOR REINFORCING COOPERATION WITH THOSE COMPANIES IT CONSIDERS TO BE ITS KEY SUPPLIERS.

The purpose of this program is to set up a network of premium alliances with key companies within Alstom's supply chain. This will help to generate a working framework to achieve common goals based on three main pillars: business development, industrial excellence and product and innovation.

This agreement, signed by Olivier Baril, Alstom's Chief Purchasing Officer (CPO) and Miguel Angel Martínez, General Manager of Intelligent Transportation System in GMV, sets out specific goals to be pursued jointly by both companies. These include access to new markets and countries, the development of tailor-made functions for multimodal transport arrangements, identification and joint development of new AVLS (Automated Vehicle Location System) functions and the development of new energy-efficiency tools and systems applied to mobility and transport systems.

Alstom and GMV have been working together now since 2014, when both companies signed a framework agreement for certifying GMV as Alstom's AVLS supplier.

GMV unveils new ITS upgrades at the latest FIAA

For yet another year GMV took part as exhibitor in the latest International Bus and Coach Trade Fair (Feria Internacional del Autobús y del Autocar: FIAA), held from 23 to 26 May in Madrid.

Under the banner "Manufacturing mobility", FIAA 2017 focused on groundbreaking road-transport solutions, in view of the upcoming overhaul of the sector on a concession basis. The event brought together authorities, politicians, distributors, manufacturers, installers and solution-providers from the road passenger-transport sector.

GMV's stand showcased its state-of-the-art technological systems, fruit of its ongoing quest for groundbreaking solutions to meet its clients' needs for different means of transport (bus, trams, BRT, etc.) and in the company's various worldwide trading areas (Europe, Asia, Africa, America). These included ***gmv planner*** as transport companies' best resource planning option, the Ecodriving System for controlling driving and energy efficiency and the Ticket Vending Machines TVM in their onboard versions and compact TVM-Mobile and TVM-Station.

GMV participates in Gijón's Sustainable Urban Mobility Plan

THE ROLLOUT OF A LOCAL CAR-SHARING SYSTEM IS AN INITIATIVE OF THE CITY COUNCIL (*AYUNTAMIENTO*) OF GIJÓN AS PART OF THE CITY'S SUSTAINABLE URBAN MOBILITY PLAN. THE AIM IS TO BOOST THE EFFICIENCY OF THE LOCAL PUBLIC-TRANSPORT FLEET AND ENCOURAGE CLEAN AND SUSTAINABLE MOBILITY. THIS PROJECT BRINGS GOVERNMENT AUTHORITIES AND PRIVATE ENTERPRISE TOGETHER IN A COMMON ENDEAVOR TO IMPROVE CITIZENS' QUALITY OF LIFE

Under this project the Ayuntamiento has replaced its old fleet of vehicles by a smaller number of shared-use vehicles (48), 14% of them electric. The vehicles of the leasing fleet have been supplied by Alphabet, a current client of GMV's fleet management and tracking service, ***MOVILOC®***.

As technological partner GMV has taken charge of setting up a vehicle booking service that also caters for shared journeys. Vehicle access is by way of a local transport card for unlocking the vehicle and starting up the engine. Fleet vehicles are fitted with GMV's U10-D onboard mobile unit and a Mifare card reader. Integration with the ***MOVILOC®*** platform enriches the system with additional report-generating and real-time vehicle-monitoring information.

In a second phase of the project, the Ayuntamiento will open up the service to certain groups of citizens who will be able to benefit also from the municipal fleet, thus improving the intermodality of the city's public-transport service.

Moviloc hailed on Transport Night

On 6 April GMV attended and sponsored Segovia's 16th Annual Transport Business Prize-Giving Ceremony (XVI *ceremonia anual del Galardón Empresarial del Transporte*). This event is organized by Madrid's Vehicle-Workshop Association (*Asociación de Talleres de Madrid*: ASETRA), an association clocking up its fortieth anniversary this year.

Held in the headquarters of the foundation called Fundación Caja Segovia, the event highlighted and rewarded the work of the most important transport firms in the region of Castilla y León.

One of the prizes handed over was the Silver Aqueduct for the Transport Firm of the Year, awarded by the Segovia Transport Entrepreneur Grouping (*Agrupación Segoviana de Empresarios de Transporte*) to the company Transalbert. The added value of this firm, specializing in the refrigerated transport of perishable freight and live animals at national level, has been the takeup of ***MOVILOC®*** , GMV's inhouse fleet-management and -tracking development.

Transalbert's aim was to find out in real time the temperature of transported freight and also the delivery time. The takeup of ***MOVILOC®*** was a resounding success; witness the award won by the firm in 2015, in the 5th ITS Prizes, awarded by the Association of New Transport Technology (*Asociación de Nuevas Tecnologías en el Transporte*).

The ***MOVILOC®*** technological solution was originally launched back in 2004. Since then it has continually been phasing in new upgrades and technological breakthroughs such as the system upgrade to favor ubiquity, incorporating an access service from handhelds (2015).

Among other recognitions and awards, in 2006 ***MOVILOC®*** won top prize in the ITS category of the International Road Federation's Global Road Achievement Awards. It has also won important international competitions in Poland, Malaysia, Morocco and Hungary.

GMV spearheads sustainable mobility

The holding of the 22nd Meeting of the Conference of the Parties (COP22) of the United Nations Framework Convention on Climate Change in Marrakech in late 2016 represented yet another sign of the Moroccan government's determination to lead, broker and support sustainable development in Africa.

For some years now, as part of this overall commitment, GMV has been a strategic supplier of technological systems for the country's main public-transport operators, such as the Moroccan multinational CityBus, the Spanish company ALSA and the Moroccan railway operator ONCF.

CityBus has recently turned anew to GMV for supply of the fleet-management and fare-collection systems for the public transport of Oujda. This Rif city, with a population of about half a million, is Morocco's eighth biggest, lying in a strategic position on the Algerian border.

The system provided by GMV for Oujda includes the state-of-the-art onboard Electronic Ticketing Machine ETC-606 plus a GPS/3G module for real-time monitoring of running times. This system will also allow passengers to pay with personalized farecards; this will come in especially handy for the many national and international students who use the system.

For some years now GMV has also been running ONCF's railway geolocation system from a modern control center in Rabat. ONCF has now reiterated its ongoing trust in GMV by awarding diverse contract enlargements, including, most notably, the equipping of 95 additional trains with the GMV-designed onboard system, the setting up of a passenger-information website and the supply of handhelds for worker alerts.

Both contract awards serve to reinforce GMV's indisputable leadership in the Moroccan transport market, where its systems have now been taken up by the urban and interurban transport of over 10 cities.

RENFE turns to GMV for improvement of the fleet management system of its freight service

RENFE MERCANCÍAS, SPAIN'S NATIONAL RAILWAY-FREIGHT SERVICE, HAS ONCE MORE TURNED TO GMV, AWARDING IT THE CONTRACT FOR UPGRADING ITS FLEET MANAGEMENT SYSTEM. WITHIN RENFE THIS IS INTERNALLY KNOWN AS ITS "*PLATAFORMA EMBARCADA DE COMUNICACIONES*" (ONBOARD COMMUNICATION PLATFORM).

Back in 2007 GMV won the contract for a first fleet-management system for RENFE's freight service. This system, completely implemented by 2011, involved fitting 387 trains with GMV's inhouse railway fleet-management technology, ***SAE-R***.

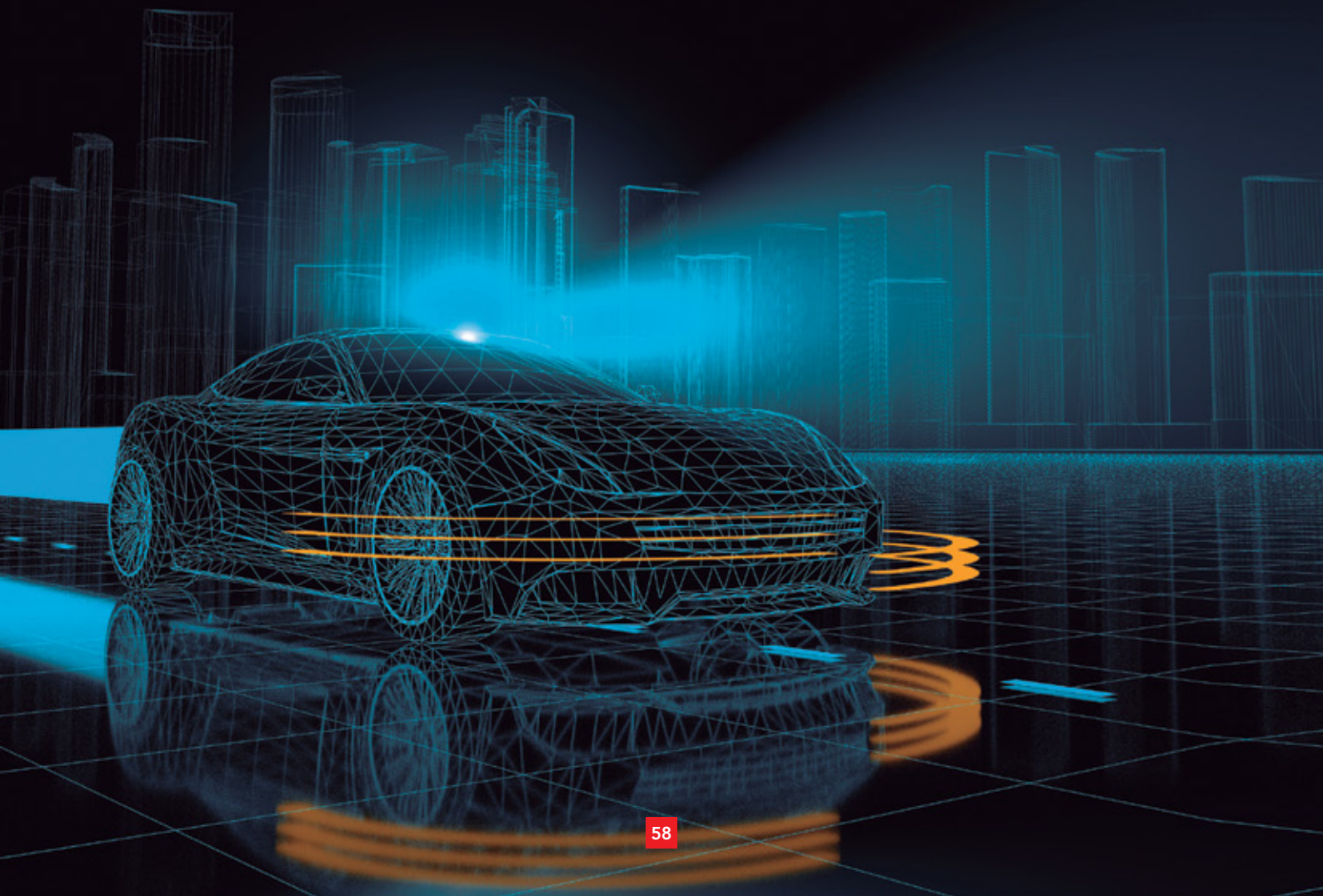
This system completes deployment of GMV's onboard system, now fitted to the whole fleet of Spain's national railway operator

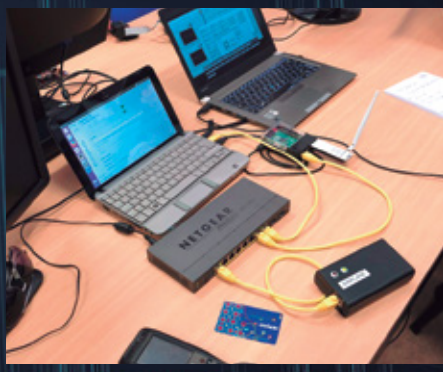
Under this new contract RENFE seeks to improve and update the system, bringing in several upgrades including complete migration of the current control center to a virtualized environment in RENFE's corporate datacenter, overhaul of the database management system plus other graphical improvements that give it a more up-to-date look. Lastly, the ***SAE-R***'s latest available technological upgrades have also been phased in, to bring the whole system into line with the new operating systems now available on the market, in order to ensure future maintainability.

This system, taken together with those already supplied for RENFE's passenger service (local, mid-distance, long-haul and high speed), completes deployment of GMV's onboard system, now fitted to the whole fleet of Spain's national railway operator (over 1800 trains and locomotives).

First results of the ENABLE-S3 automation and self-drive project

IN LATE MAY, AFTER THE PROJECT'S FIRST YEAR, A GENERAL ASSEMBLY WAS HELD OF THE ENABLE-S3 PROJECT (EUROPEAN INITIATIVE TO ENABLE VALIDATION FOR HIGHLY AUTOMATED SAFE AND SECURE SYSTEMS), PRESENTING THE FIRST DEMONSTRATORS, SIMULATORS AND VIDEOS OF WHAT WILL BE THIS PROJECT'S DEFINITIVE PLATFORMS TO PAVE THE WAY FOR AUTOMATION OF CRITICAL SYSTEMS





ENABLE-S3 is a European-Commission project co-funded by ECSEL Joint Undertaking* and awarded to a consortium of partners from more than 15 countries. Its remit is to pave the way for accelerated application of highly automated and autonomous systems in the automotive, aerospace, rail and maritime mobility domains as well as in the healthcare domain.

GMV is participating in two use cases. It is leading Traffic Jam Pilot with V2x, focusing on the automotive domain, while also taking part in the Thales Alenia-led Reconfigurable Video Processor for Space, carrying out activities centering on the space domain.

In the automotive use case GMV's activities will produce a highly automated pilot system to increase road safety, reduce congestion and benefit the environment.

In the space domain GMV will apply ENABLE-S3 methodologies to validate a technology demonstrator under extreme space conditions. This demonstrator, also resulting from this project, will involve the use of inflight-reconfigurable FPGAs to exchange vision-based navigation implementations to suit the characteristics of each phase of a space mission. In other words, reusing the same hardware to cut down costs and load. ENABLE-S3's virtual testing, verification and coverage-oriented test-selection methods will help to bring down validation costs and activities to a reasonable level, shortening the verification and validation time. This project's validation framework will guarantee European industry's competitiveness in the global automation race.

This two-day encounter served to audit and take stock of the project, selecting some of the developments to be presented to the European Commission at the end of June.

As a participant in the project GMV has taken part in the various chats to weigh up any difficulties in partners' collaborative processes observed in this first year of the project and also to define the activities that need to be tackled within the project. Together with its partners GMV has likewise taken part in the break-out sessions corresponding to its use cases.

The meeting also included a demonstrator exhibition day to showcase work and ideas as well as the state of other use cases.

ECSEL joint undertaking receives support from the European Union's Horizon 2020 research and innovation program and Germany, Austria, Denmark, Spain, USA, Finland, Czech Republic, Italy, Spain, Portugal, Poland, Ireland, Belgium, France, the Netherlands, UK, Slovakia and Norway.

GMV plays an active role in autonomous and connected car training syllabi

THE STEPS TOWARDS THE CONNECTED, AUTONOMOUS CAR ARE BEING TAKEN AT AN EVER BRISKER RATE. A WHOLE SLEW OF TECHNOLOGICAL BREAKTHROUGHS AND CHANGES ARE NOW TRANSFORMING THE SECTOR, AND NEW JOB SKILLS ARE NEEDED TO KEEP UP WITH THIS RATE OF CHANGE. EVEN MORE BREAKTHROUGHS AND ADVANCES ARE EXPECTED IN UPCOMING YEARS, SO THERE IS A PATENT NEED FOR SPECIFIC TRAINING SYLLABI TO CATER FOR THE TECHNICAL REQUIREMENTS OF A SECTOR WHERE GMV IS MASTER OF VARIOUS RELATED DISCIPLINES

In response to this new demand, the next academic year will see the introduction of the Master Degree in Connected- and Autonomous-Car Engineering, in which GMV will be playing an active part by giving lectures throughout the master-degree course. This syllabus, drawn up by Madrid Polytechnic University (*Universidad Politécnica de Madrid*: UPM) and the Automobile Research University Institute (*Instituto Universitario de Investigación y Automóvil*: INSIA), will deal with vehicle-engineering aspects, their management within the sector and the concomitant environmental impact, among other matters. It is vouched by the 25-year experience of teaching the Automobile Engineering Master Degree and 20+ years' experience in intelligent transportation systems.

GMV will help to draw up the syllabus and collaborate in matters concerning telematics, cooperative ITSs and applications of the connected- and autonomous vehicle. Special stress will be laid on practical cases involving the implementation of technologies in which GMV is past master, such as high-precision, high-integrity, safety-critical positioning for self-driving vehicles, aspects related to connected- and autonomous-vehicle Cybersecurity and specific technological solutions for applications in vehicles of this type.

Along similar lines June 17 saw completion of the second "Autonomous and Connected Vehicle Specialization Course", organized by the Spanish Automobile Professionals' Association (*Asociación Española de Profesionales de Automoción*: ASEPA) in collaboration with the University Institute for Automobile Research (*Instituto Universitario de Investigación del Automóvil*: INSIA-UPM).

This month-long course was organized in two modules, one dealing with the autonomous vehicle and the other with the connected vehicle. It involved the participation of 16 experts in these matters, including not only researchers and academics but also representatives of the main firms and cutting-edge brands in the world of autonomous and connected vehicles. GMV collaborated in this course, giving one of the lectures dealing with different cases of vehicle communication apps, offering details on a wide range of connected-vehicle services in which GMV is inputting its wealth of experience.

The Inter-American development Bank (IDB) plumps for Knowledge management

GMV has been working with the Inter-American Development Bank (IDB) to lay down the bases of a knowledge management infrastructure, doing so with the aim of furnishing users with relevant, contextual and precise information. The company used some of the best technologies for processing unstructured data: cognitive analysis, machine learning and natural language processing (NLP).

Drawing on its wealth of experience and technical knowledge, GMV's team managed to combine and adapt various solutions such as IBM Watson and Python's Natural Language Toolkit (NLTK) to come up with an answer for IDB's specific knowledge-management and information-processing needs. This includes the use of knowledge analysis engines, rule-extraction algorithms and the organization of lessons learned from past projects, as well as automatic document classification.

Javier Fernández, head of the Text Analytics & Big Data section at GMV USA, led this project, which, in his own words, has enabled GMV "*to win itself a position as leading technological partner in such a critical IDB area as Knowledge Dissemination*".

The Inter-American Development Bank is one of the main sources of long-term financing for economic, social and institutional projects of Latin America and the Caribbean. As well as granting loans, donations and credit guarantees, IBD also carries out cutting-edge research projects to find groundbreaking and sustainable solutions for this region's most urgent problems. Set up in 1959 to speed up progress in its member developing countries, IDB strives daily to improve peoples' lives.

GMV used some of the best technologies for processing unstructured data: cognitive analysis, machine learning and natural language processing (NLP)

RENLand distinguished with an Esri SAG Award

THE GIS PROJECT DEVELOPED BY GMV FOR *REDES ENERGÉTICAS NACIONAIS* (REN), A PORTUGUESE COMPANY WHOSE MAIN BUSINESS ACTIVITY IS RUNNING THE COUNTRY'S PUBLIC POWER DISTRIBUTION SYSTEM, HAS RECENTLY WON A SAG AWARD. THE SAG AWARD (SPECIAL ACHIEVEMENT IN GEOGRAPHIC INFORMATION SYSTEMS) HAILS THE YEAR'S MOST IMPORTANT, INNOVATIVE AND IMPACTFUL PROJECT

RENLand's main mission is to manage the vegetation growing in the right of way of power lines and gas pipelines and Grupo REN's other properties, through the monitoring and registration of activities using a mobility solution.

RENLand consists of a collaborative solution that makes teamwork more agile and efficient, facilitating data-gathering and information sharing. Following a long-term business partnership between GMV and ESRI, RENLAND has been developed using ESRI's most recent technology in the field of Geographic Information Systems (GIS). RENLand is an innovative concept dreamed up by REN's Property and Right of Way managers, concerning operational management and maintenance of the right of way of power lines and gas pipelines run under REN's responsibility.

The award was handed over during the Esri User Conference held in San Diego, California between 10 and 14 July

GMV supports the IE Data Expedition 2017

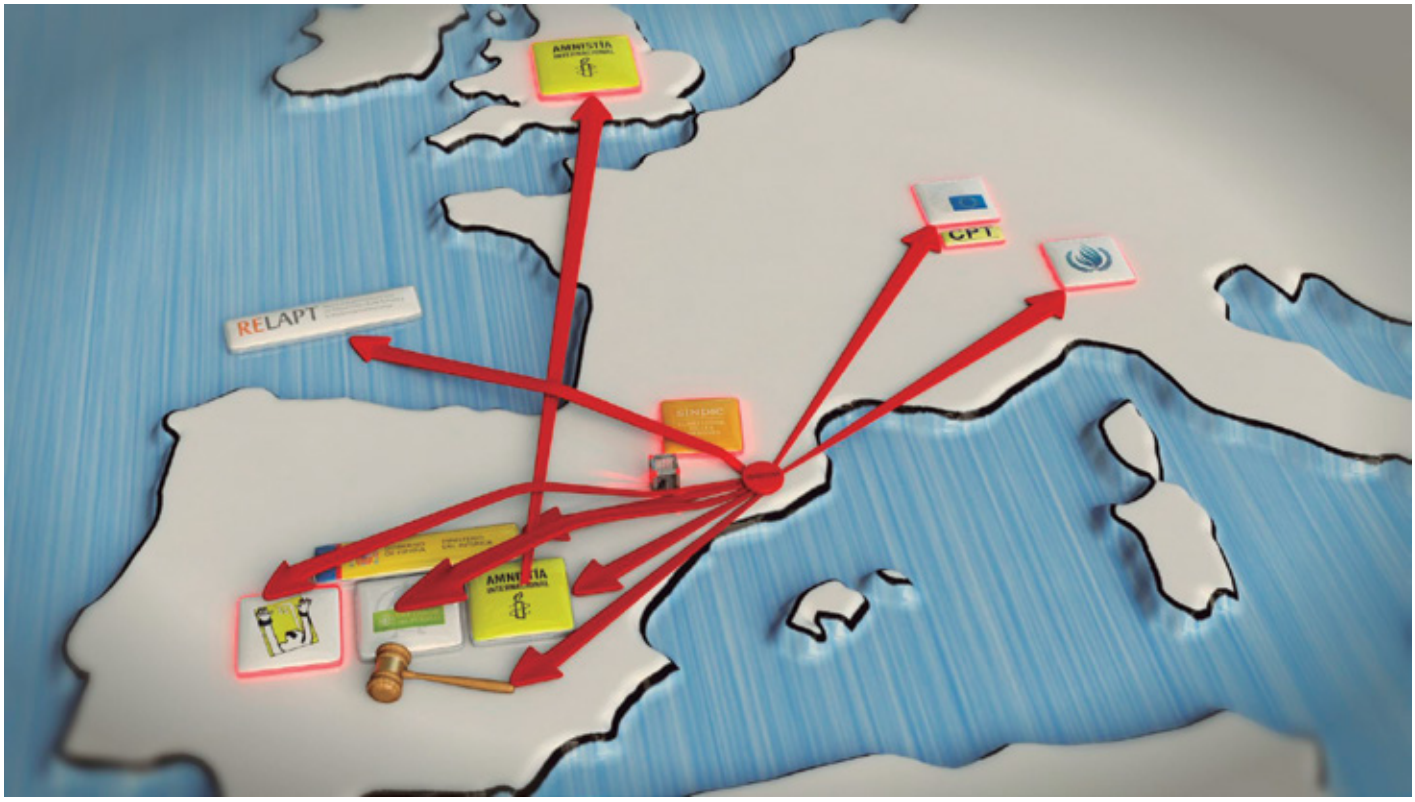
FOR YET ANOTHER YEAR GMV HAS SUPPORTED AND SPONSORED "IE DATA EXPEDITION 2017", A DATATHON ORGANIZED BY THE BIG DATA CLUB OF THE SPANISH BUSINESS INSTITUTE (INSTITUTO DE EMPRESA: IE)

For two days the participants, mostly students of IE's Big Data MSc, took on the challenge of solving a real business case for the Inter-American Development Bank (*Banco Interamericano de Desarrollo*: BID), doing so by analyzing data furnished by the bank itself. This analysis was to show how expert knowledge is spread throughout the various BID departments and the degree of collaboration between them. The teams were free to choose such tools as they thought fittest for the tasks in hand, although they were encouraged to use graph-based models.

GMV, on the strength of its vast data-analysis experience, was invited to collaborate in the event. Federico Sembolini, GMV Data Scientist, took part as mentor while José Carlos Baquero, division head and leader of GMV's Big Data group, acted as a jury member. GMV is currently leading Big Data and Business Analytics initiatives in areas such as Cybersecurity, fraud prevention, healthcare, Industry 4.0 and precision agriculture.

The IE is recognized as one of the world's finest business schools. It offers the highest level of education and an international environment with students from all around the world. The competition attracted a very high technical level and turned out to be a very positive and enriching experience both for the event organizers and the participants.

Barcelona University's Human Rights and Penal System Observatory launches a pioneer website in Europe



BARCELONA UNIVERSITY'S HUMAN RIGHTS AND PENAL SYSTEM OBSERVATORY (*OBSERVATORIO DEL SISTEMA PENAL Y LOS DERECHOS HUMANOS*: OSPDH) HAS SET IN MOTION THE INSTITUTIONAL VIOLENCE COMMUNICATION AND REGISTRATION SYSTEM (*SISTEMA DE REGISTRO Y COMUNICACIÓN DE LA VIOLENCIA INSTITUCIONAL*: SIRECOVI), DEVELOPED WITH GMV TECHNOLOGY

■ SIRECOVI is a trailblazing European website that enables victims, informers and human-rights organizations to report abuse through a private communication channel on a web platform. Cases of institutional violence in prisons, police stations, probation centers, juvenile facilities, foreigner internment centers or certain activities of security forces on the public thoroughfare can now be reported easily and confidentially. GMV has developed this platform according to such aspects as security, user-friendliness, accessibility and, above all, data confidentiality, safeguarding at all times the privacy of the persons involved.

GMV has guaranteed the protection of confidential data with the overriding aim of safeguarding at all times the privacy of the persons involved

SIRECOVI allows social organizations and the public at large to report any alleged case of institutional violence and also shows how to activate the corresponding victim-protection protocols. It will also help in OSPDH research, providing a database for the study of institutional violence and mapping the various cases.

SIRECOVI does not in any way replace the due procedural mechanisms or stand in for the judiciary. Rather is it a new mechanism provided by OSPDH to forestall any cases of violence perpetrated by state officials or private security guards carrying out public functions.

This system has been set up with the backing of the City Council (Ayuntamiento) of Barcelona and has been made possible by an agreement reached between the OSPDH and the Catalan Lawyers' Board (*Consell de l'Advocacia Catalana*), representing Catalunya's 14 professional lawyers' associations.

Innovation Ecosystem and Industry 4.0

THE INNOVATING COMPANIES FORUM (*FORO DE EMPRESAS INNOVADORAS*: FEI) HAS ORGANIZED THE EVENT "INNOVATION ECOSYSTEM AND INDUSTRY 4.0" TO TACKLE THE SPANISH INDUSTRIAL FABRIC'S PERCEIVED NEED OF TRANSFORMATION AND MODERNIZATION.

The event was opened by Juan M. Vázquez, Secretary General of Science and Innovation at Spain's Economics Ministry, Francisco Marín, Director General of Spain's Industrial Technology Development Center (*Centro para el Desarrollo Tecnológico Industrial*: CDTI) and Luis Fernando Álvarez-Gascón, General Manager of GMV Secure e-Solutions and Vice President of FEI.

The meeting stressed the industrial fabric's need of transformation and modernization, with particular emphasis on the connection between industry and science. In pursuit of this overall goal, speakers highlighted the need of taking stock of the current situation and generating innovation policies to suit, doing so by means of an ongoing debate with the main stakeholders and representatives of the ecosystem surrounding industry.

Luis Fernando Álvarez-Gascón pinpointed the sheer speed of change as the characteristic feature of the Industry 4.0 transformation. He therefore argued that Spain needed to make a special effort to keep up a high rate of change to enable the country to reach the 4.0 welfare level.

Pursuit of the top welfare level calls for a reinvention of itself by Spain's industrial sector, accepting the need for taking on a reindustrialization process to boost the sector's GDP contribution. This should be done, moreover, not only by developing technology-based companies but also by taking the 4.0 revolution even into the primary sector.

The FEI Vice President and CEO of GMV Secure e-Solutions also argued that Spain has to increase its R&D investment level on the strength of bigger contributions from both the public and private sectors. He went on to advocate, "*an accompanying debate about the policies and instruments best suited to optimize the results of Spain's investments*".

For his part Juan M. Vázquez, Secretary General of Science and Innovation at Spain's Ministry of Economics, Industry and Competitiveness, expressed his conviction that a bigger R&D allotment and an increase in company investment will boost the industrial sector's GDP contribution.

TECHFEST: Driving technology and data management

Data are an increasingly prized and coveted source of information in the business world. Many researchers are now working flat out to extract information of interest, helping in decision-making procedures and bringing great benefits to companies and institutions.

On 2 to 4 May the Higher IT Engineering School of Valladolid Polytechnic University (*Escuela Técnica Superior de Ingeniería Informática de la Universitat Politècnica de València*: ETSINF-UPV) held TechFest 2017. This conference brought together top Big Data professionals to speak about current trends and recent breakthroughs.

Carlos Sahuquillo, GMV's Cybersecurity consultant, member of the ISACA Valencia Chapter and the Cloud Security Alliance, was one of these keynote lecturers, giving the paper "*What use do companies make of our data?*" Carlos explained what type of information is kept by major firms on each one of us and with what purpose (sometimes simply to improve their service, other times for advertising purposes and yet others to earn money from this data). "*In the future we will have proactive medicine drawn from the data captured daily by monitoring devices, wristband activity trackers and intelligent watches*" explained Sahuquillo.

The event's prime aim was to drive technology and data management in the upcoming generations of IT-, robotics- and electronics-professionals. Lectures, chats, workshops and competitions involving open data and related technologies made up the activity schedule of TechFest, an event organized by the Chair of Transparency and Data Management.

PRODUCTIO, CDTI's GMV-led project, kicks off

GMV IS LEADING THE CONSORTIUM, WHICH IS FOCUSING ON RESEARCH INTO NEW TECHNOLOGY TO IMPROVE INDUSTRIAL MAINTENANCE PROCESSES, WHICH HELP TO FORECAST ANOMALIES AND FAULTS, REDUCING DOWNTIME AND INCREASING MACHINE AVAILABILITY

PRODUCTIO (*PROductivity InDUstrial EnhanCement through enabling TechnlOgies*) is a project involving a multi-sector and multidisciplinary national R&D consortium with the aim of "*researching into diverse technologies, techniques, tools, methodologies and knowledge intended to increase the operational capability of industrial processes (Overall Equipment Efficiency: OEE) in the context of interconnected industry 4.0*", in the words of Miguel Hormigo, GMV's Industry 4.0 Project Manager. The project will facilitate the adoption of maintenance and productive solutions in interconnected industry and encourage digital confidence by means of new security approaches.

The kick-off meeting has recently been held, inaugurated by Luis Fernando Álvarez-Gascón, CEO of GMV Secure e- Solutions, chaired by Miguel Hormigo, Southern-Region Manager of GMV Secure e-Solutions and with the presence of several CEOs and innovation managers of the participating firms: Gonvarri, Fagor Arrasate, Hiperbaric, Zener, Industria PuigJaner, Tecnomatrix and some of the collaborating companies and organizations like the Technological Institute of Castilla y León (*Instituto Tecnológico de Castilla y León*), Tecnalia, Eurecat and Ikerlan.

GMV is leading said consortium, which is focusing on research into new technology to improve industrial maintenance processes, which help to forecast anomalies and faults, reducing downtime and increasing machine availability. Technology like artificial intelligence in predictive maintenance of blanking line facilities; predictive and assisted maintenance for maintaining machines distributed throughout the world; trailblazing manufacturing technology related to interconnected industry 4.0 that supports decision-making in the production and maintenance phase; forecasting of system faults and formulae for boosting the overall efficiency of industrial-process using Big Data analytical tools; in short, gleaning knowledge for turning machines/tools, firstly, into cyber-physical systems that can improve aspects of reliability, performance, availability, productivity and quality; and, secondly, into technology for ensuring the integrity of sensor data and heading off fraudulent use.

As Miguel Hormigo stressed, "*this project will pool the particular goals of participating firms and organizations around a core of common interest: boosting the productivity and competitiveness of Spain's industry while converting the project into an Industry 4.0 benchmark*".

GMV is participating in two of the sixteen projects approved by Spain's Industrial Technology Development Center (*Centro para el Desarrollo Tecnológico Industrial*: CDTI) in its 2016 call of the Strategic Program of National Business Research Consortia (*Programa Estratégico de Consorcios de Investigación Empresarial Nacional*: CIEN), which finances large-scale experimental industrial R&D projects carried out collaboratively by business groupings.

The project will facilitate the adoption of maintenance and productive solutions in interconnected industry and encourage digital confidence by means of new security approaches

ANTONIO LOZANO LIMA

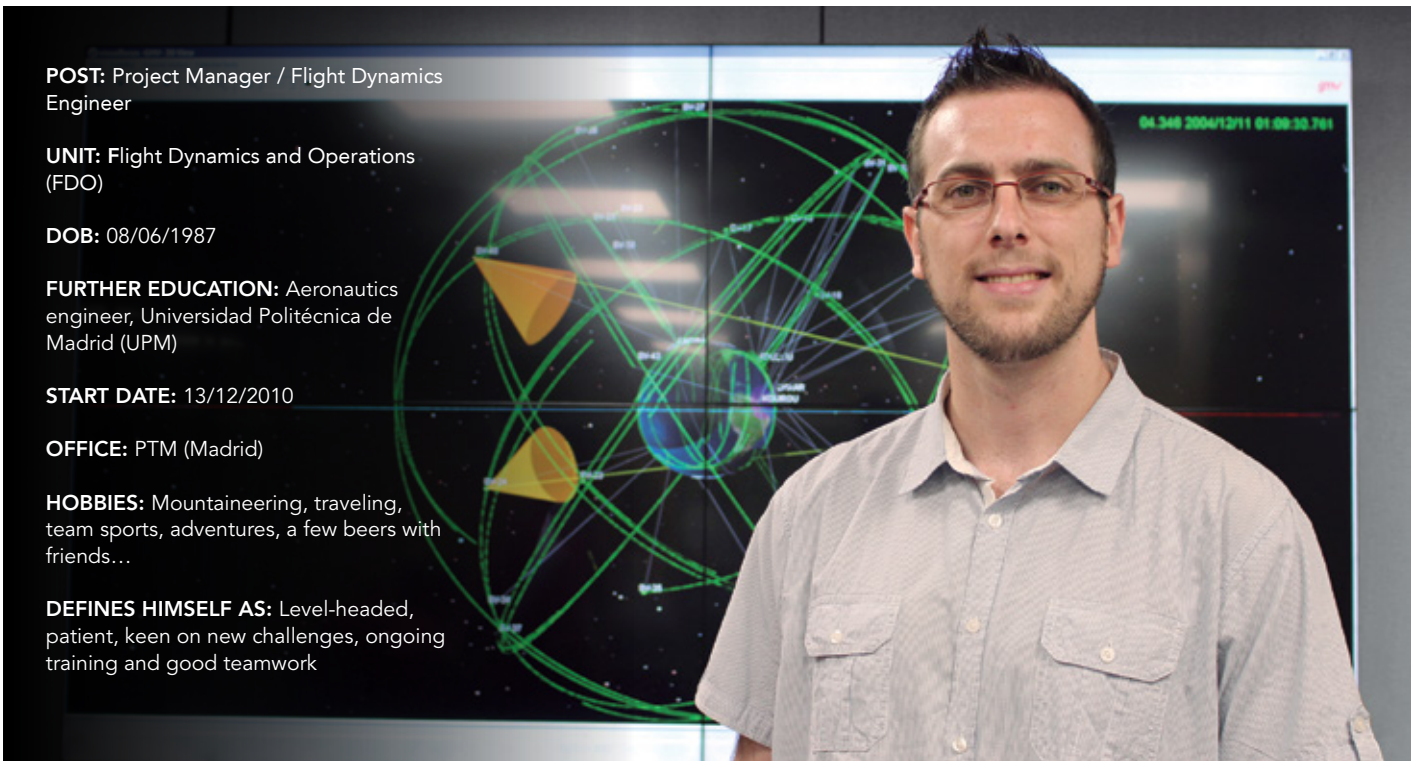
"GMV's internships are full of opportunities, not only for the firm but also the students involved"

In summer 2009, when I still had a year of my degree course left, I was specializing in the study of airports, a subject that had always interested me; at that time I had never considered working in space. On the other hand, I saw it as essential to gain some experience of the working world before ending my degree and closing off other options too soon. I therefore decided to look for summer jobs in the various areas of aeronautics and ended up here after seeing an announcement on the university notice board.

It still surprises me to think that two months of half-day working were enough to change my years-long preferences, but here I found something different, more than just an interesting job. The working environment was great, for sure, collaborating with a young, go-getting team and seeing how everything worked so smoothly at all company levels. At that time I didn't realize just how much work went into achieving this surface serenity but I soon sensed that here there were many merit-worthy ideas buzzing around.

Apart from this whole GMV context, the internship itself was a great experience. You start out with stereotyped ideas of churning out the photocopies,

Antonio Lozano with the 2017 intern intake



POST: Project Manager / Flight Dynamics Engineer

UNIT: Flight Dynamics and Operations (FDO)

DOB: 08/06/1987

FURTHER EDUCATION: Aeronautics engineer, Universidad Politécnica de Madrid (UPM)

START DATE: 13/12/2010

OFFICE: PTM (Madrid)

HOBBIES: Mountaineering, traveling, team sports, adventures, a few beers with friends…

DEFINES HIMSELF AS: Level-headed, patient, keen on new challenges, ongoing training and good teamwork

Internships enable us to reboot and conduct small research projects in fresh areas

getting coffees for the boss and being bored out of your mind. Instead of this you find out from the very first day that everything has been laid on for you; you're given induction presentations about the firm; you're offered several work areas to choose from and you're guided by tutors who take a real interest in you. It was truly a fantastic professional and personal experience. Encouraged by my tutors and the whole inspirational experience, I decided to continue as intern during the last year of my degree while doing my honors thesis. When the moment came to graduate and look for my first job, the decision was a done deal: I wanted to join GMV.

I joined the Flight Dynamics and Operations (FDO) department, where I'm still working today, developing orbital dynamics software. Among many other interesting things, this job has given me the chance to work with people from various countries, to collaborate in our clients' satellite mission analysis and participate in various satellite launches from the mission control center. Apart from the work itself, I also like to take every chance to join in GMV's many sporting activities (soccer, basketball, volleyball) where you can have a good time, keep fit and get to know colleagues from other departments.

After a few years I was given the chance to act as an internship tutor and I didn't hesitate for one moment. Internships enable us to reboot and conduct small research projects in fresh areas; this is a great attraction, without any doubt. They also represent a great chance for the company to find good candidates for future vacancies. But for me it's also a chance to continue the task of bringing GMV to greater notice and passing on all the pluses that convinced me to stay with the firm. Since then I've been lucky enough to tutor several company internships, with over 10 undergraduates from various degrees and universities. Every second spent on this activity has been well worthwhile. Many of these former interns are now my colleagues and friends in GMV, and I hope there'll be many more in the years to come.

GMV IN THE WORLD

COLOMBIA
Edificio World Trade Center Bogotá - Calle 100 No. 8A-49. Torre B. PH.- 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
GMV Insyen AG.
- 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.: (+60 3) 9205 7788 Fax: (+60 3) 9205 7788

NORTH AMERICA
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, California 90014
Ph.: +1 (310) 728-6997 Fax: +1 (310) 734-6831

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

PORTUGAL
Avda. D. João II, N° 43 Torre Fernão de Magalhães, 7° 1998-025 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

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

Juan de Herrera n°17 Boecillo - 47151 Valladolid
Ph.: +34 983 54 65 54 Fax: +34 983 54 65 53

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

Balmes 268-270 5ª Planta - 08006 Barcelona
Ph.: +34 93 272 18 48 Fax: +34 93 215 61 87

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

Edificio Sorolla Center, Av. Cortes Valencianas n°58, local 7 - 46015 Valencia
Ph.: +34 96 332 39 00 Fax: +34 96 332 39 01

Avenida José Aguado, 41 - Edificio INTECO, 1ª Planta - 24005 León
Ph.: +34 91 807 21 00 Fax: +34 91 807 21 99

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

UNITED KINGDOM
Harwell Innovation Centre, Building 173, 1st floor, suite C131 & C134 Curie Avenue, Harwell
Science and Innovation Campus, Didcot, Oxfordshire OX11 0QG
Ph.: +44 1235 838536 Fax: +44 (0)1235 838501