Press Release

Holistic Approach for a secure last line of defense

Houston, TX, USA, February 12, 2018

At the ARC Industry Forum which was held in Orlando, Florida, from February 12 – 15, HIMA presented its comprehensive functional safety concept which offers maximum security by expanding the scope from the safety instrumented system to its security-relevant environment.

The future of the process industry is digital. Digitization holds many opportunities for plant operators to enhance efficiency, increase flexibility and make their plants future-proof. At the same time, the growing level of automation and connectivity can be a door-opener for serious threats to plant security. In recent years, large-scale professional cyberattacks and chip hardware vulnerabilities affecting industrial plants around the globe have clearly shown the need for the process industry to take cybersecurity seriously. At the ARC Industry Forum, HIMA safety experts explained why plant operators should implement a holistic functional safety approach that ensures plant security in times of increasing cybercrime.

In late 2017 a safety controller deployed in a Middle East process facility was successfully hacked. The safety instrumented system (SIS) was compromised and initiated a plant shutdown. While no damage or injuries occurred, the incident should serve as a wake-up call to heighten awareness of cybersecurity in the industry as it was the first publicly-known successful attack on a safety instrumented system – which is the last line of defense in any process plant. Furthermore, critical hardware vulnerabilities affecting most modern processors have recently been identified. Attack modes such as Meltdown and Spectre exploited these in order to steal data from computers all around the world.

“In both of the above-mentioned cases, HIMA safety controllers were not affected. But we take these incidents very seriously and work hard to always be one step ahead,” Dr. Alexander

Horch, Vice President Research, Development & Product Management at HIMA comments: “It is important to note that there is no such thing as 100% guaranteed safety or security. But by choosing the HIMA holistic functional safety approach which protects the core SIS as well as its environment, plant operators get the maximum level of safety and security possible.”

The purpose of modern functional safety solutions is to reduce safety and security risks to a minimum. Therefore, a holistic approach is needed which not only includes the core SIS (final control elements, logic solver incl. I/O module and sensors), but also its environment like the engineering station, asset management tools (AMS) and handhelds as well as field entry panels and HMIs. By complementing the SIS with the “HIMA Security Environment for Functional Safety,” this approach takes all important security-relevant aspects of industrial control systems (ICS) into account. These include the five following areas: Controller hardware and firmware, engineering toolkit, PC infrastructure, communication infrastructure and lifecycle management.

In terms of firmware, a dedicated operating system specifically developed for safety-critical applications runs on HIMA safety controllers. The HIMA firmware, which is 100% HIMA software, provides an extremely low software error rate and has no backdoors implemented. It is impossible to access the program code during operation as application programs run within a container and no other parts of the CPU firmware can be accessed. On the hardware side, unused Ethernet ports can be disabled and/or locked physically. Thanks to the total separation of SIS and basic process control functions and systems (BPCS) according to the requirements of the standards for functional safety (IEC 61511) and automation security (IEC 62443), no common cause failures can occur.

When it comes to the engineering, HIMA works with its own, single-purpose engineering tool SILworX, again 100% HIMA software. This solution offers various security features such as two-factor authentication for project and controller data, a well-defined user management including security admin role as well as functional blocks with password protection (locking/read-only), just to name a few. By monitoring the application program via system variables, SILworX is even able to detect changes and to issue an alarm in case unauthorized changes are made.

Also, the communication infrastructure has to be secured. The HIMA security environment relies on the proprietary protocol for controller communication SafeEthernet, and the communication stack is Achilles certified by Wurldtech. Separated protection layers between

CPU and COM modules lead to an absence of feedback. Networks are clearly separated via firewalls and demilitarized zones, and the controller is tap-proofed to prevent ARP spoofing.

For an effective cyber-defense, the PC infrastructure should be set up with a secure BIOS management, reduced access rights and with only the required Windows services activated. Office laptops should not be used as engineering stations. The engineering station should be kept completely separate. The PCs should feature an intelligent password management system and work with a minimal set of application programs only.

Last but not least, the lifecycle management has to take security into account, too. HIMA safety systems have received various security certifications such as Achilles, ISASecure, EDSA and TUV. The ISO 27001 certification for HIMA's information security management systems (ISMS) is ongoing. HIMA also carries out penetration tests together with customers, service providers and universities. Development takes place in a dedicated network, and access to source codes is strictly restricted and supervised. In standardization organizations like IEC and OpenGroup, HIMA experts are proactively driving safety and security standardization forward.

"Security is an integral part of HIMA services and engineering. In addition to cyber-secure hardware and software, we provide security awareness training, basic security checks of HIMA safety systems, product security training and security lifecycle services," explains Dr. Horch.

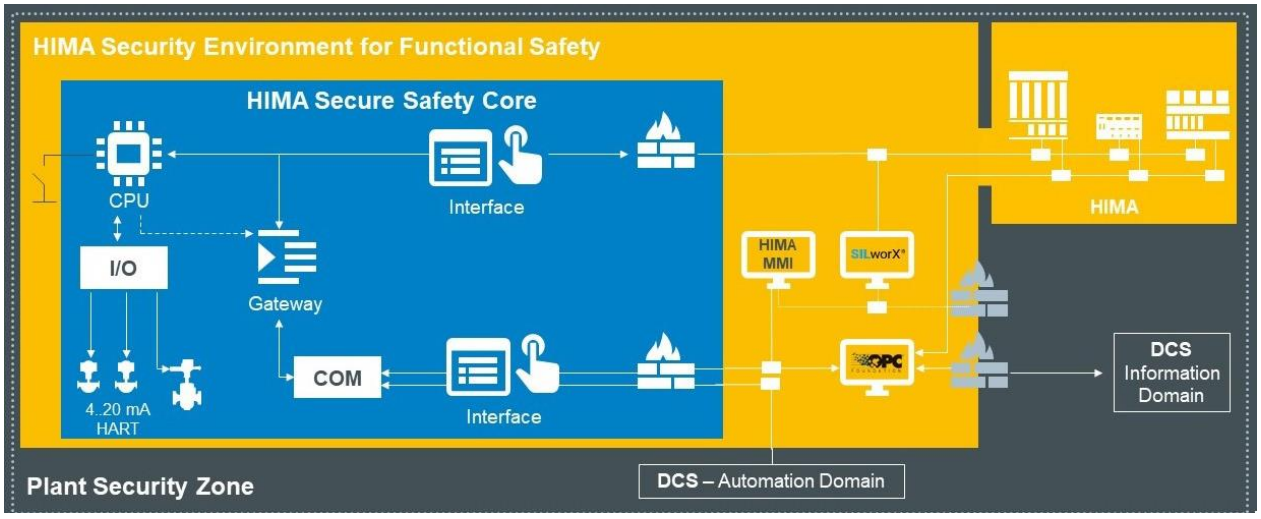

Image 1: The "HIMA Security Environment for Functional Safety" takes all important security-relevant aspects of industrial control systems (ICS) into account.

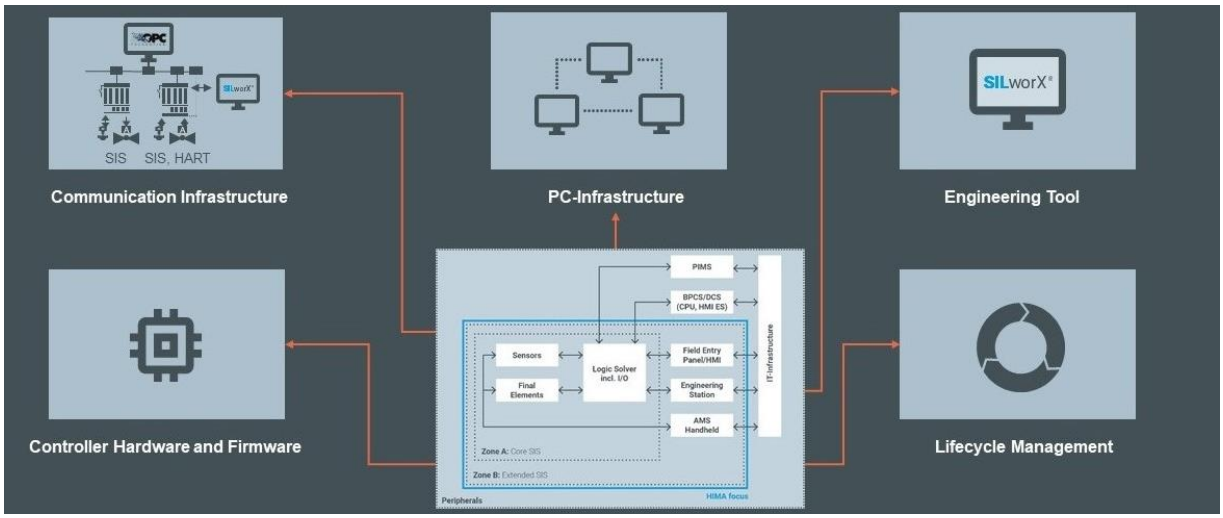

Image 2: Security in ICS depends on five areas.

Image 3: Dr. Alexander Horch, Vice President Research, Development & Product Management at HIMA.

Images © HIMA Paul Hildebrandt GmbH

About HIMA

The HIMA Group is the world's leading independent provider of smart safety solutions for industrial applications. With more than 35,000 installed TÜV-certified safety systems worldwide, HIMA qualifies as the technology leader in this sector. Its expert engineers develop customized solutions that help increase safety, cyber security and profitability of plants and factories in the digital age.

For over 45 years, HIMA has been a trusted partner to the world's largest oil, gas, chemical, and energy-producing companies. These rely on HIMA solutions, services and consultancy for uninterrupted plant operation and protection of assets, people and the environment. HIMA's offering includes smart safety solutions that help increase safety and uptime by turning data into business-relevant information. HIMA also provides comprehensive solutions for the efficient control and monitoring of turbomachinery (TMC), burners and boilers (BMC) and pipelines (PMC). In the global rail industry, HIMA's CENELEC-certified SIL4 COTS safety controllers are leading the way to increased safety, security and profitability.

Founded in 1908, the family-owned company operates from over 50 locations worldwide with its headquarters in Bruehl, Germany. With a workforce of approximately 800 employees, HIMA generated a turnover of approximately €126 million in 2016. For more information, please visit: www.hima.com

HIMA has operated in the Americas since the early 1980s. Its headquarters for the Americas is located in Houston, Texas. Discover more at www.hima-americas.com

Press contact HIMA Americas
HIMA Americas Inc.
Nicole Pringal
Sr. Marketing and Public Relations Manager

5353 W Sam Houston Parkway N., Suite 130
Houston, Texas 77041, USA
Phone +1 713 482 2069 I Cell +1 713 876 9828
npringal@hima-americas.com

www.hima-americas.com

Press contact HIMA Headquarters
HIMA Paul Hildebrandt GmbH
Daniel Plaga
Group Manager Global PR

Albert-Bassermann-Straße 28
68782 Bruehl
Phone: +49 6202 / 709-405
Fax: +49 6202 / 709-123
E-Mail: d.plaga@hima.com

www.hima.com