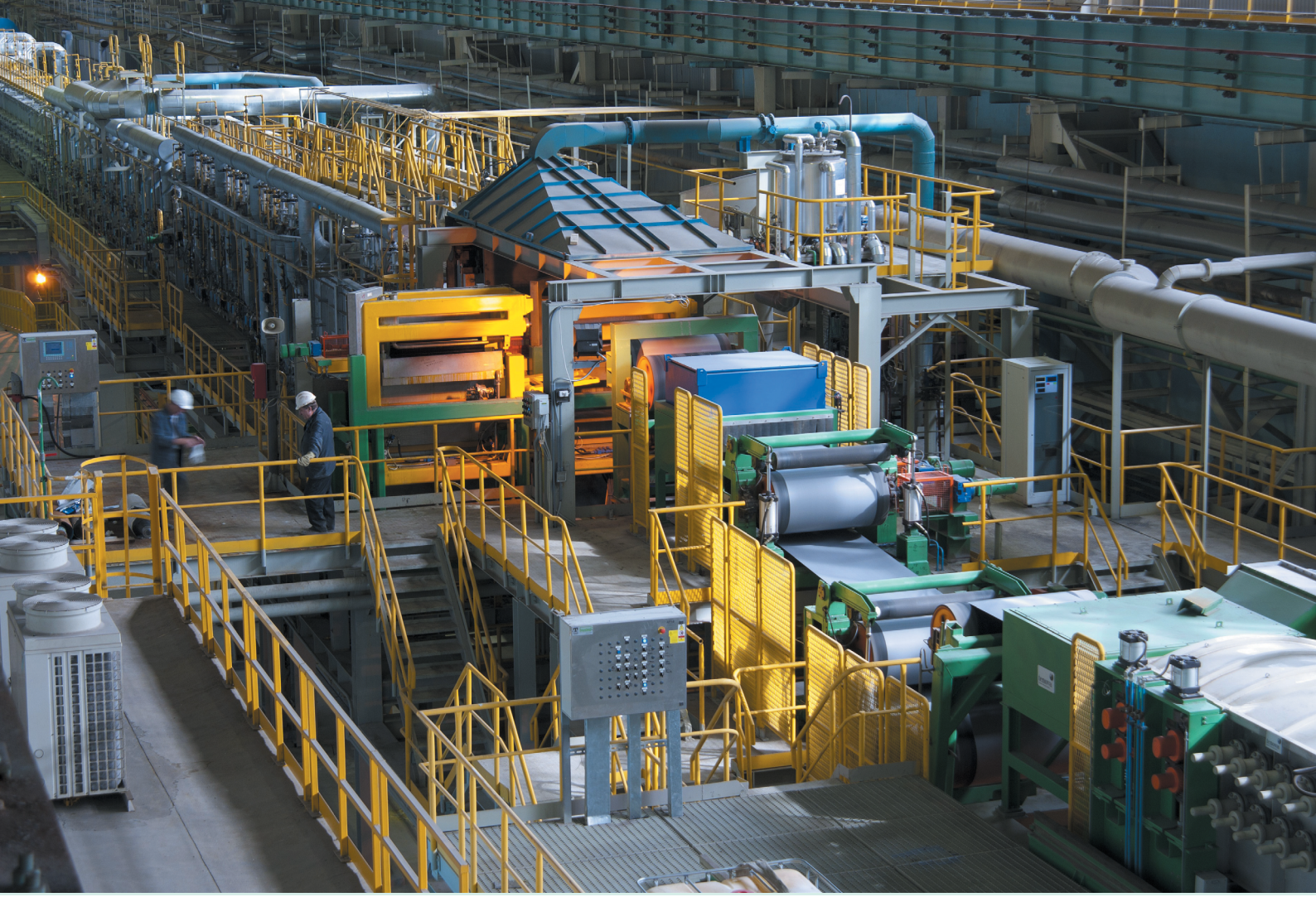


Kaspersky Industrial CyberSecurity passes industrial infrastructure pilot test at NLMK

kaspersky

Kaspersky Industrial CyberSecurity

NLMK

https://www.nlmk.com/en/

Ferrous metallurgy

- Established in 1934
- Part of the NLMK Group of companies
- Lipetsk, Russia
- Share in Russian steel production: 18%
- Production capacity: more than 13 million tons of steel a year

Novolipetsk Steel, or NLMK, is the main production site of the international NLMK Group, one of the most cost-efficient metallurgical companies in the world, with a vertically integrated business model and assets in Russia, Europe and North America.

Thanks to self-sufficiency in basic raw materials, energy and advanced technologies, NLMK Group is the leader of Russia's metallurgy industry and the only Russian company among the world's top 20 largest steel manufacturers. The Group's steel production capacity exceeds 17 million tons per year.

The NLMK plant produces about 80% of all NLMK Group's steel production. Production at Novolipetsk Steel includes all stages of the industrial process: from processing raw materials to the production of high-grade steel. The high-quality steel products of NLMK are used in various industries, ranging from construction and engineering to power equipment and offshore wind farms.

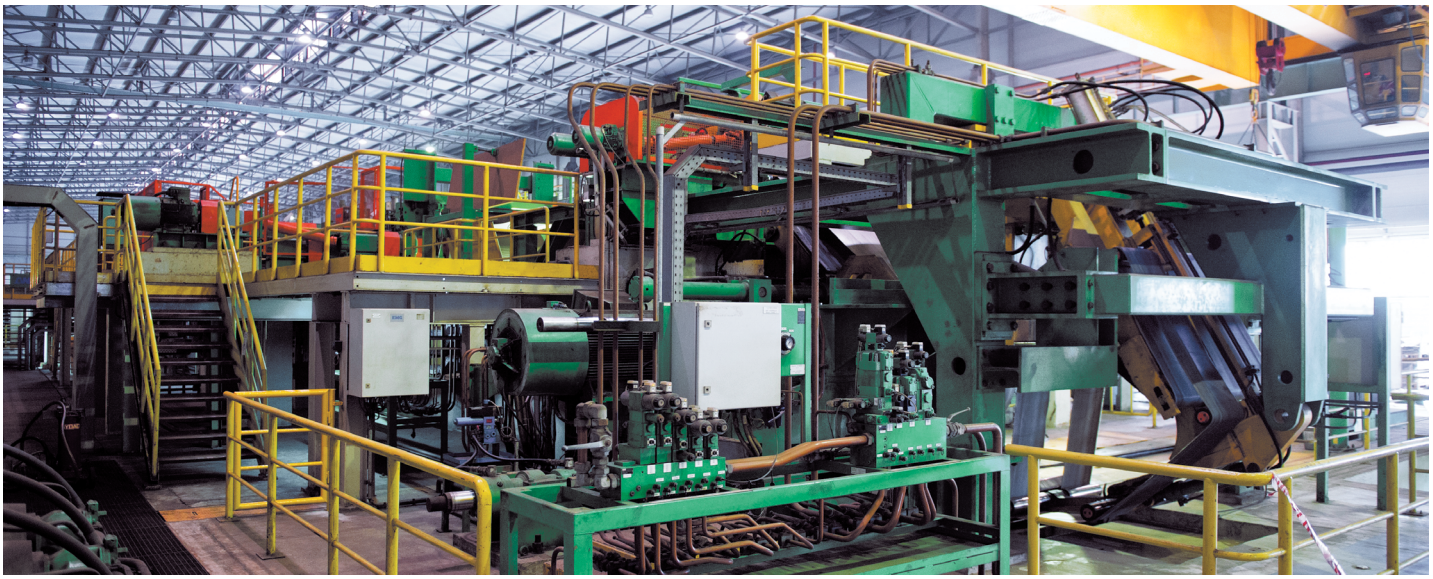
Challenge

NLMK, together with Kaspersky, launched a pilot project to create effective protection of industrial control systems (ICS) from cyberattacks in the electrical steel shop.

During project implementation, NLMK carried out the task of creating a modern automation infrastructure combining the computing resources of industrial control systems (ICS) in several territorially distributed data centers. This approach increases the reliability of the automation systems and reduces maintenance costs. At the same time, this architecture makes it possible to form a clear network perimeter and organize the secure transfer of data from automation systems to corporate networks, thus increasing the resilience of ICS to cyberattacks.

"The project to secure NLMK's infrastructure was a valuable and unique experience. The use of virtualization at the upper level of the ICS presented some interesting technical tasks, which Kaspersky experts successfully solved. Such challenges undoubtedly have a positive impact on the development of our solution, and we are always ready to cooperate with such customers."

Georgy Shebuldayev,
Head of Kaspersky Industrial CyberSecurity.



Non-intrusive solution
Kaspersky Industrial CyberSecurity does not affect the operational continuity or consistency of industrial processes.

Real attack scenarios
The technologies integrated in Kaspersky Industrial CyberSecurity have been developed based on the real-life scenarios of cyber-physical attacks on different industries.

Risk management
Implementation of a comprehensive cybersecurity solution in an industrial environment helps improve an enterprise's risk management system.

Solution

To ensure cybersecurity inside the perimeter, NLMK chose Kaspersky Industrial CyberSecurity, a set of technologies and services designed to secure operational technology layers and other enterprise elements, including virtualization servers, engineering workstations and PLCs.

The technologies behind Kaspersky Industrial CyberSecurity not only protect endpoints but also detect intrusions and anomalies in industrial networks with the help of passive monitoring.

"For us, the project to secure NLMK's infrastructure was a valuable and, in some respects, unique experience. The use of virtualization at the upper level of the ICS presented some rather interesting technical issues," said Georgy Shebuldayev, Head of Kaspersky Industrial CyberSecurity. "For example, deploying several virtual servers on one physical hypervisor imposes additional requirements in terms of security and load balancing. When antivirus scanning starts on several virtual servers, the increased total load on the hypervisor can affect the performance of the other virtual machines and, ultimately, the industrial processes. Kaspersky experts coped successfully with all the challenges posed by the infrastructure, which was by no means typical for an industrial customer."

All the components of Kaspersky Industrial CyberSecurity were successfully tested and are now undergoing user testing in the steel shop.

"Cooperation between NLMK and Kaspersky will not be limited to this pilot project – it is the beginning of a promising technology partnership."

Sergey Slauta,
Director for Automation of Industrial Processes at NLMK.

Results

"Implementation of modern intelligent automation systems in production increases the risks of potential cyberattacks, which can affect the industrial process. To prevent them from occurring at NLMK, we are introducing integrated echeloned protection at the automation infrastructure level," commented Sergey Slauta, Director for Automation of Industrial Processes at NLMK. "Kaspersky Industrial CyberSecurity addresses the real needs of our enterprise and meets our main cybersecurity requirements for industrial processes. I'm sure that cooperation between NLMK and Kaspersky will not be limited to this pilot project – it is the beginning of a promising technology partnership."

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization - including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers - without impacting on operational continuity and the consistency of industrial process.

Learn more at www.kaspersky.com/ics

Kaspersky ICS CERT:
https://ics-cert.kaspersky.com
Cyber Threats News:
www.securelist.com

#Kaspersky
#BringontheFuture

www.kaspersky.com



* World Leading Internet Scientific and Technological Achievement Award at the 3rd World Internet Conference

** China International Industry Fair (CIIF) 2016 special prize