TANECO

TANECO protects vital oil production

kaspersky

Kaspersky Industrial CyberSecurity

TANECO

http://www.taneco.ru/en

Energy, Oil & Gas

- Established: 2005
- Nizhnekamsk, Republic of Tatarstan, Russia
- Subsidiary of Tatneft Group
- Uses Kaspersky Industrial CyberSecurity

Prompt detection of cyber threats targeting programmable logic controllers helps to enhance overall protection of the process control system.

TANECO is a Russian oil refining company and part of the $15 billion Tatneft Group. The company was created in 2005 to drive oil and petrochemical production in the Tatarstan region of the country. It is the first industrial facility of its scale built from scratch in post-Soviet Russia.

The project continues to increase production, contributing significantly to the Tatarstan economy. By unit capacity, Tatneft is now Russia's largest oil refinery.

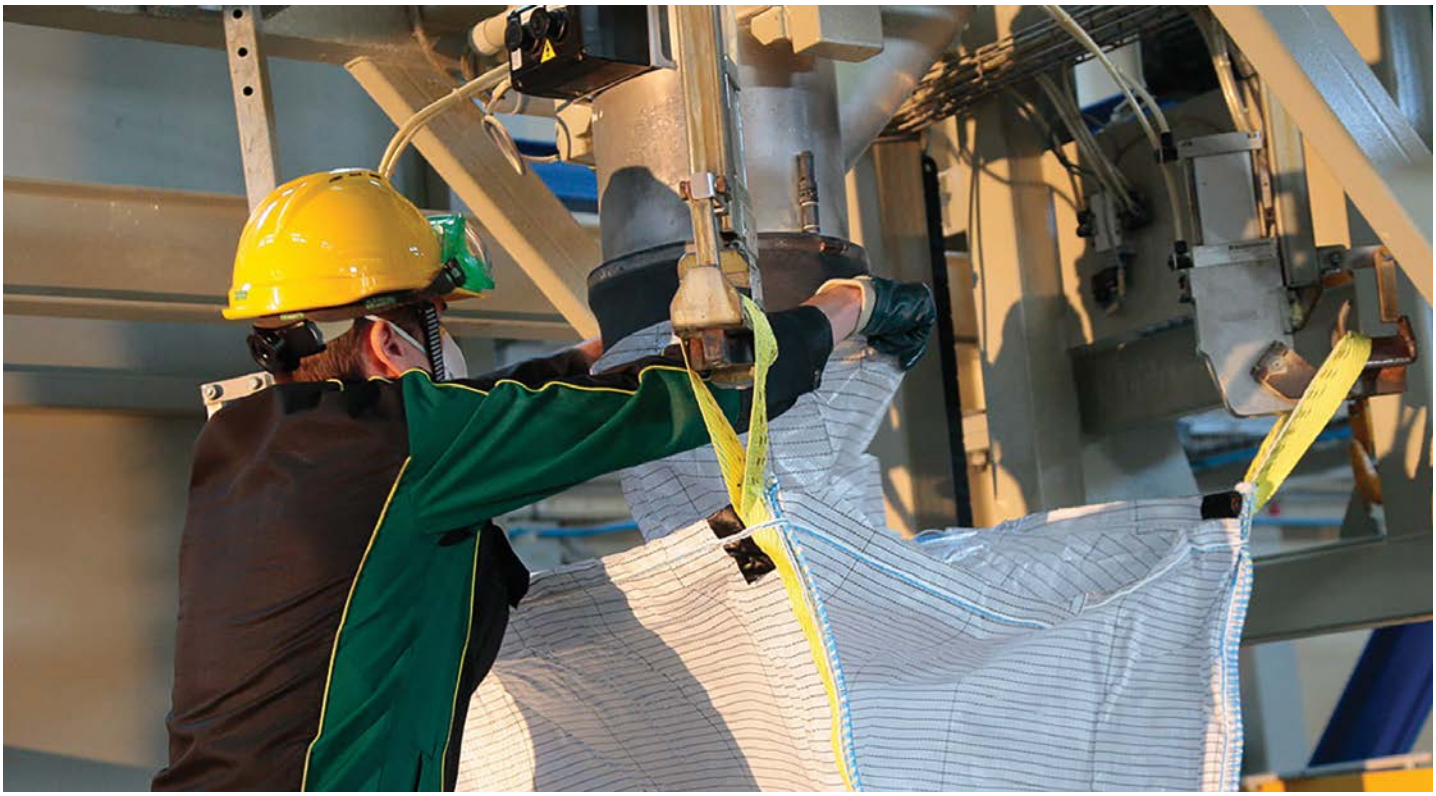
The next phase of development will see TANECO expand its mix of petroleum products in line with international production standards and environmental compliance.

TANECO's strategy is to focus on hi-tech, efficient and environmentally friendly oil refining processes. The company plans to create a range of oil-based products, strengthening vertical integration within the Tatneft Group.

Challenge

TANECO's success is heavily reliant on the continuity of manufacturing processes. The company uses industrial control systems (ICS) to deliver a technology edge over the competition and minimize production costs.

However, the growing level of production automation and the use of technologies originally designed for corporate networks in its industrial infrastructure have exposed the company to the risk of cyber-attacks.



> “The performance of Kaspersky Industrial CyberSecurity exceeded all our expectations. Just months after deployment, the solution detected an unauthorized connection attempt by an outside laptop to one of the controllers.”

Marat Gilmutdinov,
Head of Industrial Control Systems Department, TANECO

TANECO initially brought in Kaspersky to audit the IT security of its rail discharge terminal handling vacuum gas oil (VGO) supplies. Kaspersky was then challenged with implementing a pilot project to demonstrate cyber security functionality for operator/engineering workstations and SCADA servers. Part of the cybersecurity system would also need to monitor the integrity of the industrial network and control the critical parameters of the process flow.

The requirements also stated that the solution should not interfere with the existing industrial control system.

The Kaspersky solution

Marat Gilmutdinov, Head of Industrial Control Systems Department, TANECO, says the business has worked with Kaspersky for years: “We’ve relied on Kaspersky for many years to protect our corporate network. We didn’t think twice when it came to choosing who to trust with the information security of our industrial facilities.

“Having analyzed the potential threats faced by hi-tech oil refineries, we opted for the Kaspersky Industrial CyberSecurity solution by Kaspersky. It was important for us to buy a solution developed domestically by a vendor capable of providing prompt assistance with any possible issues during deployment and operation.”

Security
Detection of various system commands for programmable logic controllers (PLC) protects against cyber-attacks targeting key assets of the industrial control system

Control
Detection of unauthorized devices provides rigorous and efficient control over the industrial network

Results

Gilmutdinov says the project to secure the VGO discharge terminal was completed successfully, with Kaspersky experts working alongside TANECO's in-house team: "The capabilities of Kaspersky Industrial CyberSecurity exceeded all our expectations. Just months after deployment, Kaspersky Industrial CyberSecurity detected an unauthorized connection attempt by an outside laptop to one of the controllers. The attackers were attempting to modify the operation settings of a sensor.

"The project demonstrates that solutions like this can be used successfully with industrial facilities. TANECO plans to further expand cooperation with Kaspersky in providing security for its industrial networks."

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


CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

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

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