ACTEMIUM Slovakia

SAFE AND RELIABLE

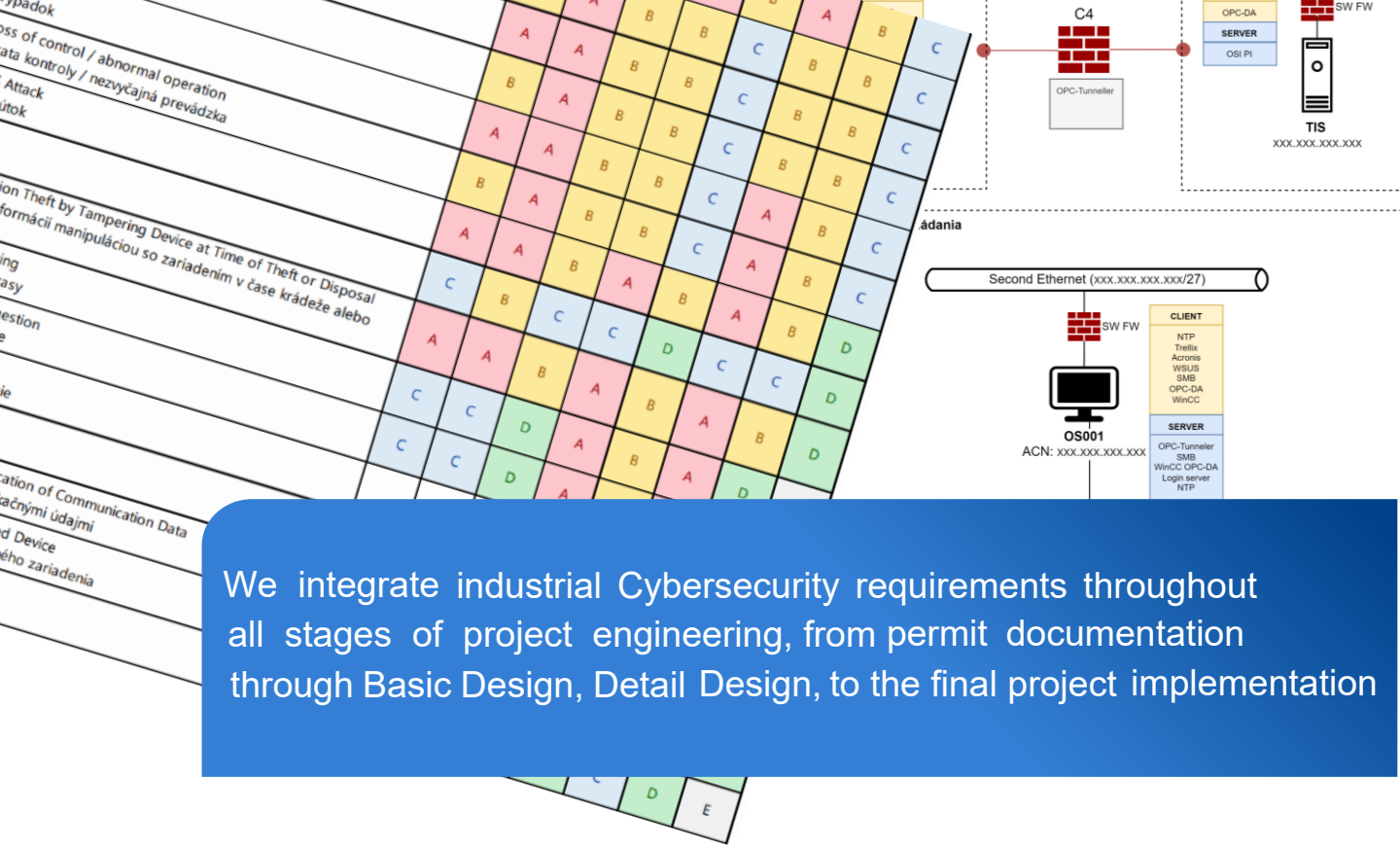
We specialize in **cybersecurity** of industrial control systems. The implementation of our projects complies with **IEC 62443** and Slovak legislation, especially the NIS, NIS2/CER and Cyber Security Act.

Our goal is to ensure that every operation works **efficiently and safely.** We transform complex standards and legislative requirements into straightforward, pragmatic and implementable solutions. The proven cybersecurity implementation process consists of three logical phases:

1. Development of comprehensive security documentation
Preparation of complex cybersecurity project documentation in accordance with the IEC 62443 standard, forming the basis for subsequent implementation.

2. Technical implementation and integration
Implementation and integration of designed technical, process and organizational measures in strict compliance with the project documentation for cyber security.

3. Verification, validation and continuous improvement
Documentation of implemented asset configurations, evaluation of the achieved level of security against set objectives and development of recommendations for continuous improvement of cybersecurity.



We integrate industrial Cybersecurity requirements throughout all stages of project engineering, from permit documentation through Basic Design, Detail Design, to the final project implementation

We believe that the foundation of a robust and auditable cybersecurity management system in the OT environment is **precise project documentation.**

Our solutions:

- Extensive inventory and accurate identification of all OT infrastructure components.
- Systematic risk management, which includes threat analysis, vulnerability identification, impact assessment and probability assessment.
- Network segmentation according to the Purdue model in compliance with the principles of zones and interconnections to increase security.
- Determination and assessment of security levels (SL-T /SL-A) for individual zones and connections, in order to achieve the required level of security.
- Hardening of systems according to manufacturer recommendations or CIS standards for OT environments.
- Identity and access rights management based on clearly defined roles and the principle of minimized privileges.
- Protection against cybersecurity threats using certified solutions designed for OT environments.
- Management and implementation of control system component updates
- Configuration of network components in compliance with the architecture of zones and interconnections.
- Monitoring of OT network through passive systems integrated with SIEM.
- Backup management with a focus on minimizing the time required to restore operations.

ProCS, s.r.o. has been presented under the **Actemium brand** since 2015, as a part of the international **VINCI Energies group.** Actemium is an international network focused on industrial processes. Actemium designs, implements and maintains its customers' production facilities in order to improve their performance and competitiveness.

CONTACT
ProCS, s.r.o.
Kráľovská ulica 8/824
927 01 Šaľa
Slovakia

web: https://www.actemium.sk
e-mail: info@actemium.sk
LinkedIn: https://linkedin.com/company/actemium-slovakia