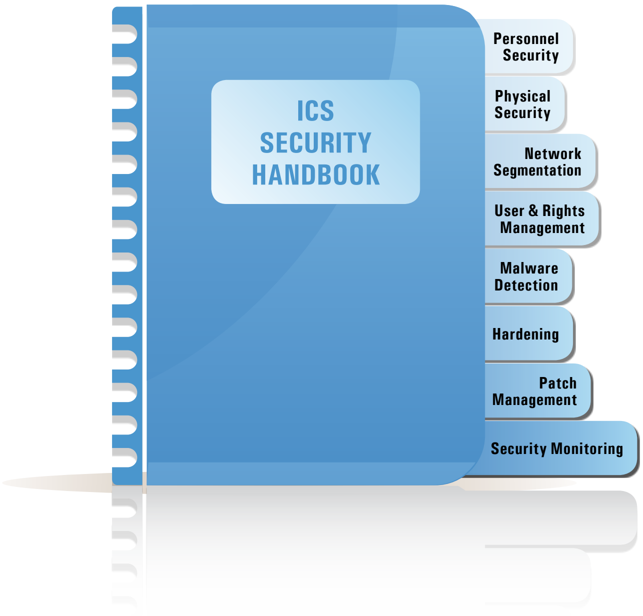
Choose certainty.
Add value.

# Security Handbook for ICS Manufacturers

## An integrated approach to IT Security

Manufacturers of Industrial Control Systems (ICS) have to recognize rising IT Security threats in the industrial environment. Moreover, threats to security can potentially become relevant for safety. Given this, vendors implement an increasing number of security mechanisms aimed at overcoming these threats and risks. However, operators and system integrators also have to be aware of IT Security to reach an appropriate level of security for the whole system, e.g. control center and ICS. A state-of-the-art approach is the defense-in-depth strategy, which provides for the implementation of security measures at different levels and zones of the IT infrastructure and system as a whole (as shown in the figure below). The defense-in-depth strategy is covered by a Security Handbook supplied to the ICS operators by the ICS manufacturer. The Security Handbook has to be adjusted to the operator´s plant environment.

## Security Handbook



TÜV SÜD Group

www.tuev-sued.com/embedded

### Addressed security issues

Topics addressed by the Security Handbook must include the following (see figure above):

**Personnel Security:** Skilled and regularly trained personnel, job descriptions include security issues.
**Physical Security:** Protection against damage from fire, flood, earthquake, dust, pressure, temperature extremes etc., security measures for off-premises equipment.
**Network Segmentation:** Technologies like firewalls, VLAN and VPN.
**User and Rights Management:** Defined security roles and responsibilities of employees and contractors, effective authentication and authorization mechanisms.
**Malware detection:** Updated anti-malware software, exclusion of critical components.
**Hardening:** Secure configuration, disabling of unnecessary functions, services, protocols and ports.
**Patch Management:** Knowledge of relevant patches and their impacts, risk assessment, testing, system observation after implementation.
**Security Monitoring:** Security logging, analysis and alarming, defined severities, established security incident handling process.

To protect ICS, security mechanisms must be implemented and maintained at ICS, communication and platform level. Policies and guidelines must support compliance, governance and implementation.

### TÜV SÜD – expertise for the power networks of tomorrow

Represented at over 600 locations worldwide, TÜV SÜD is your experienced partner for networking IT solutions in office and industry.

**Our services at a glance:**

- **Support:** Delivering a first draft of the security handbook which we then adjust to the manufacturer's requirements and hence the operator's plant environment
- **Analysis:** Deriving appropriate security measures to ensure secure operation of the manufacturer's ICS
- **Development:** We work with the manufacturer to compile a well-structured security handbook from draft to final version

**Contact us today – our experts will be happy to assist you with detailed advice:**

**Your contact:**
**Dr. Thomas Störtkuhl**, Product Manager Industrial IT Security
TÜV SÜD AG Embedded Systems
+49 89 5791-1930
Barthstr. 16
D-80339 München
Thomas.Stoertkuhl@tuev-sued.de