



# Industry Profile Energy Systems



## Reliable energy systems on the highest level

Thanks to state-of-the-art energy systems, such as powerful emergency power generators, the energy supply in power plants is reliably guaranteed even if the external power supply fails. These systems ensure that operations can continue smoothly or that an orderly shutdown process can be initiated. Our innovative controllers and control units, which have been developed in accordance with the highest international standards for functional safety, guarantee maximum availability and efficiency. We rely on clearly defined, certified processes that are implemented strictly in accordance with IEC standards.

## Safety and security for power plants

Protecting power plants against unauthorised access or targeted external attacks is a key component of seamless security of supply. We support power plant operators and energy suppliers as a reliable partner by developing and maintaining high-availability access control systems. These systems ensure protection even in the most sensitive and critical areas of energy supply, such as nuclear power plants.

With our customised security solutions, we make a decisive contribution to ensure that the energy infrastructure is comprehensively protected at all times - for a secure future for your energy systems.

## Scope of Services

- Process control according to IEC 61508 and IEC 60880
- Realization of development tasks in all project phases
- Preparation of the FMEA / FMECA for the hardware and software used
- Development of safety concepts

## Safety & Expertise

With our comprehensive expertise in the areas of safety and security, we support our customers from the initial idea through to the successful implementation of their projects. Whether in cooperation with you or independently in our company - we offer customised solutions that meet the highest safety requirements.



## Specific Project Experience

- System and software engineering for emergency diesel generator engine controllers
- Development and maintenance of access control systems
- Requirements engineering at system and software level for safety-critical engine controllers
- Test management at system and unit level
- Development of an ID card issue and access control system with client-specific optimization of the system
- Implementation of the safety requirements according to client's and BSI-IT guidelines – reinforcement of systems
- Maintenance and support for this system (server and workstation hardware and software), focusing on operational reliability and maximum availability
- Support for the client's network topology
- Requirements analysis of customer specific safety requirements in the 'access control' business process and IT
- Consulting regarding the BSI fundamental security, IT-Grundschutz Catalogues

## Systems Engineering

- Requirements engineering at system level
- System design / architecture
- Preparing the system development plan
- Analysis and consulting for the selection of server technologies focusing on client's needs
- Interfacing heterogeneous periphery components
- Interfacing the access control system with the client's higher-level plant systems

## Software Development

- Requirements engineering at software level
- Software architecture design
- Implementation in various optimally suitable languages and use of appropriate frameworks on different OS platforms
- Simulation of interfaces and system and periphery components
- Model-based development

Standards	
KTA1401	EN 50133 / DIN VDE 0830 Part 8
IEC 60880	IEC 61508
Analysis of safety requirements	
<ul style="list-style-type: none"> <li>• BSI 'IT-Grundschutz Catalogues'</li> <li>• SEWD IT guideline</li> </ul>	

## Functional Safety

- Support for / preparation of the system FMEA

## Support Processes

- Configuration management
- Problem and change management
- Tool development and tool management
- Tool qualification
- Development of simulation environments

## Verification and Validation

- Preparation of module tests
- Preparation of software integration tests and software tests
- Preparation of system integration tests and system tests
- Preparation of the test documentation
- Creation of automated test sequences (module, integration, software and system tests)
- Test and risk management
- Analyses
  - Static code analyses
  - Code reviews
  - Dynamic code analyses
  - Compiler analysis report
  - Compiler failure report
  - Coverage analyses (MC/DC etc.)
  - WCET analysis
  - Stack use analysis
  - Runtime error analysis
- Reviewing all results from the development process

## Tool Experience (synopsis)

- Jira, confluence, git
- MKS/PTC
- Enterprise Architect
- Matlab, Simulink
- Esterel SCADE, MTC, QTE, KCG
- Eclipse
- Diab C Compiler, CompCert
- AbsInt a (aiT, Stack), Astrée
- Lauterbach Debugger
- Vector CANalyzer
- Cantata++
- NI TestStand