VICCON

CONSULTING

Energy Security Management

An innovative approach for the further development of security management in the energy sector

IMPRINT

Brochure: Energy Security Management - An innovative approach for the further development of security management in the energy sector

DIGITAL TRANSFORMATION

The energy transition, characterized by the switch to renewable energies, essentially means a shift in the generation of energy from centralized to decentralized units.

Energy in the context of this document refers to generation, transport, trade, distribution and use of energy. For this purpose, business processes and infrastructures are available that are organized centrally or decentrally. The energy sector is European, including the procurement of raw materials, it is even internationally networked. It encompasses conventional raw materials such as coal, gas or nuclear fuels as well as renewable energies such as water, wind or sun. It has strong political and security significance for nation states. Thus, the sector is highly regulated and often entirely or partially in the hands of the state.

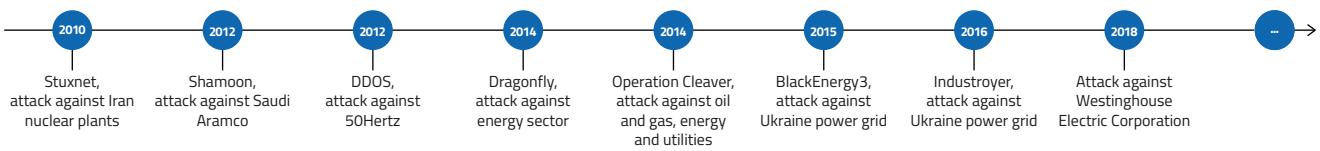
The energy transition, characterized by the switch to renewable energies, essentially means a shift in generation of energy from centralized to decentralized units. The progressing decentralisation of energy production, storage and trading calls for networked and digital control as well as for increasing data exchange. Connectivity grows with each digital component, whether in the power plant or at home. It also means shifting power generation from large power plant turbines to multiple spread power generation. This shift comes with the growing fact that energy security less and less depends on systems that work according to physical and deterministic laws, but depends increasingly on information technology systems that do not have these properties, do not have the degree of reliability and rather have a probabilistic nature due to their inherent weaknesses. Whereas analogue systems in conventional and nuclear areas used to be designed to last 30 to 40 years, today, digital components removed from the manufacturers maintenance schemes after 10 years. Without support and maintenance, IT-based systems cannot be operated safely in the long term. The Internet of Things (IoT), machine and automation-based networking of devices bring more flexibility and efficiency, but at the same time new flaws and threats. Everything is connected to everything in terms of information technology. The frequent lack of technical maturity of digital systems, the lack of long-term design of components and the vulnerability of inherent systemic or IT flaws present an enormous challenge for the entire energy industry during digital transformation.

CYBER ATTACKS

Since energy supply is one of the critical infrastructures, it is an interesting goal for professional non-state and state actors. The sabotage of energy infrastructures by cyber-attacks is a possible scenario, and in the case of electricity has regional, national or, due to the European electricity network, also transnational effects.

In the past, repeatedly "cyber accidents" showed up, i.e. the contamination of systems with malware due to inadequate internal processes, but also successful cyber-attacks carried out by hacker groups on IT of energy supplier. The latter consists of systems supporting business processes, the so-called Business IT, as well as operating resources for energy supply, measurement, control and regulation systems, often also referred to as Operational IT (OT). Particularly well-known are the attacks on the Iranian nuclear facilities (Stuxnet) and the attacks on the Ukrainian power grid (BlackEnergy3, Industroyer), both of which penetrated the OT and caused considerable damage.

Possible attack scenarios in the energy sector, however, do not only refer to attacks on central components or control systems. In the electrical power sector, attacks on a large number of IoT devices that control power in households, or on a certain number of electrically powered cars during the charging phase, or on a certain number of photovoltaics or wind turbines, are also conceivable. Such attacks aim to bring the entire power grid to a blackout. Due to the lack of large power plant turbines, which can compensate for certain fluctuations within the power grid through the laws of physics, such as inertia of mass, this capacity will no longer exist in the future and will have to be compensated through intelligent IT logic. For this reason, the mere consideration of cyber security within individual companies is of little help. If energy security is to be achieved, it must be organised in the energy ecosystem, for example at the European level.



PLANT AND GRID SECURITY

In order to ensure safe operation, holistic approaches are required

Safety means the protection of people and the environment. Security means the protection against malicious actions. Data protection or User Data Privacy protects personal data from misuse. For the operating mode of nuclear reactors, transformer stations or pipelines, digital components that control valves, measure and regulate pressure or switch lines are necessary. Such components must be protected on site by adapted object protection, yet must also be adequately protected against cyber-attacks notably in the context of a networked and digitized infrastructure.

Not only the EU Single Market with its European Energy Exchange EEX, but also many energy system transition projects require connectivity between the parties involved and massive data exchange, for example for billing, maintenance or forecasting purposes. An HVDC converter site, which is functionally similar to a transformer station, requires several dozen 19" cabinets of digital equipment to operate – this brings about totally new requirements for the operators as this creates attack vectors and attack paths that did not exist before. In order to guarantee secure operation and rule out the possibility that IT components become attack means, attack routes or targets, holistic approaches and methodologies, cross-company structures and interactions as well as cooperation between all parties involved in the energy sector and on its borders, such as the automotive industry, are required.

Plant and Grid Functional Safety	Plant and Grid Operations	User Data Privacy
Plant and Grid Security		

ENERGY SECURITY MANAGEMENT

VICCON pursues a overarching approach in the form of an Energy Security Management System® (ESMS) for energy suppliers which takes the ecosystem into account.

Although the energy sector is regulated and the parties concerned are interconnected through energy infrastructures, there is no strong cooperation across the sector. There is no uniform understanding of the significance, setup and structure of a security management system. For this reason, new approaches and ideas are currently being discussed as to how cross-company security management can be achieved. The need is entailed by the necessary interaction of different company units, the common objective of physical protection, functional safety as well as connectivity and fusion of digital systems with business IT. Thus, a security management approach is sought that combines the areas of business, system management, communication and decentralized infrastructures. At the same time, there are numerous requirements that can arise, for example, from data protection, certification or compliance audits such as ISO 27001, IT security catalogue or SEWD-IT. In addition to that, there are European or international frameworks and standards.

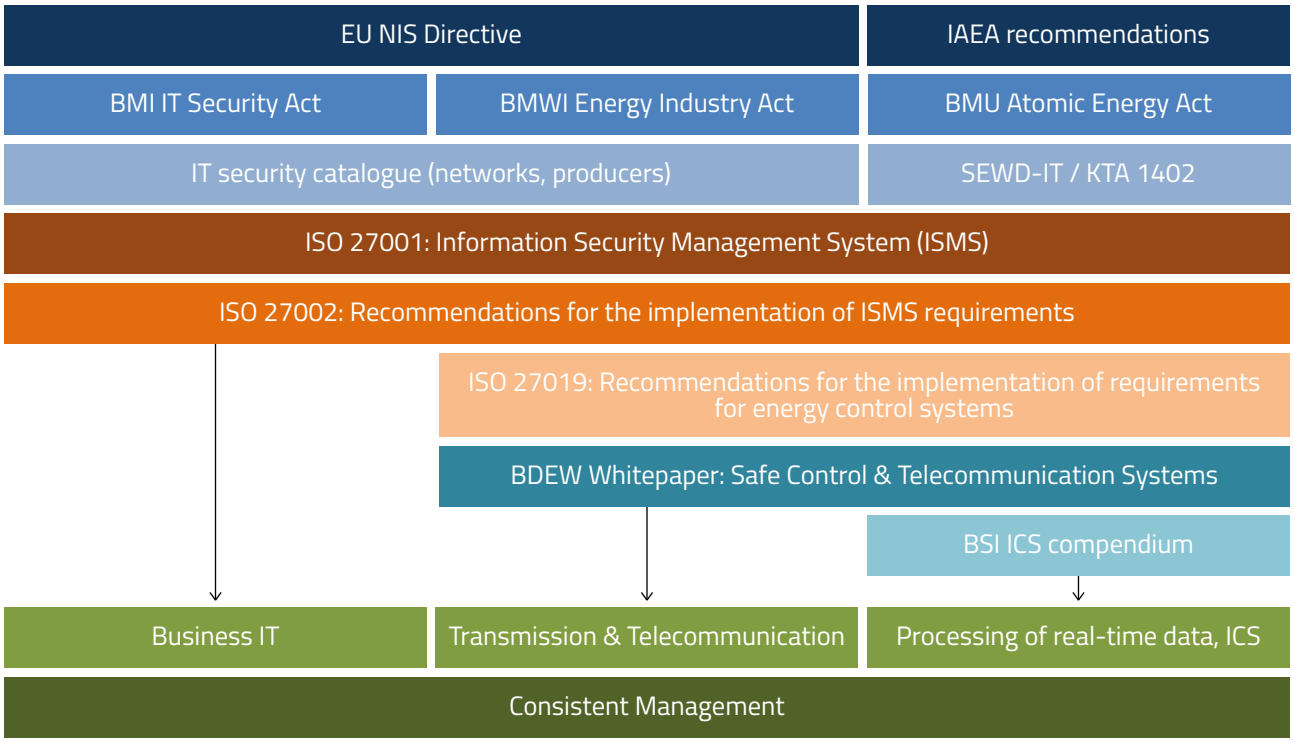
VICCON follows a comprehensive approach by means of an Energy Security Management System® (ESMS) for energy suppliers which takes the ecosystem into account. The supply of energy is supported by various digital system environments that closely interact with business processes. A common and efficient protection across all business units, supply infrastructures and sites should be provided in order to achieve the overall goal of a secure digital supply. To this end, existing and future standards for cyber security and information security will be linked and implemented.

Energy Security Management System®			
Business Process Information Security			
Business IT	Communication	Operation	Support & Maintenance
Protection of IT Systems	Protection of Telecommunication Systems, WAN	Protection of Control Systems, Safety Systems, Operational Systems	Protection of Operational Systems, Maintainance Data

DIGITAL TRUST AND SECURITY STRATEGY

Regulation in the energy sector is strong in most nation states, especially when nuclear energy is part of the energy production. In Germany, various authorities are involved in the regulation of IT security in the energy sector in order to create the necessary trust within the population (see below). In the future, European and international organisations will also gain more influence on the harmonisation of IT security and will perpetuate and better enforce rules for minimum standards and cooperation.

Trends and topics such as industry 4.0, digital trust, resilience, networked society and new work must be incorporated into future reflections. VIC-CON processes such requirements in a security strategy from which concrete measures for the future work of the security departments and the entire company are generated with a methodical approach.



ADVICE - DIALOG - KNOWLEDGE TRANSFER - IMPLEMENT - EDUCATE

For about 20 years, VICCON has supported organizations in understanding security-relevant developments, building up the necessary know-how and processes for them, thus allowing them to control them securely.

With you and in dialogue with all company levels, VICCON develops ideas and seeks a suitable orientation for the security policy in the light of the different requirements.

VICCON develops strategies for secure and resilient organizations, follows the digital transformation and advises on the implementation of these strategies in the form of Next Generation Security Management.

VICCON pursues the goal of strategically anchoring security in the company according to management and business policy. Particular emphasis is placed on information security management, the management of cyber risks as well as prototype and know-how protection.

CONTACT

For further information please contact us:

VICCON GmbH

Ottostrasse 1
76275 Ettlingen
Germany

Phone: +49 7243 719734
Fax: +49 7243 719704

E-mail: info@viccon.com
www.viccon.com

VICCON

CONSULTING