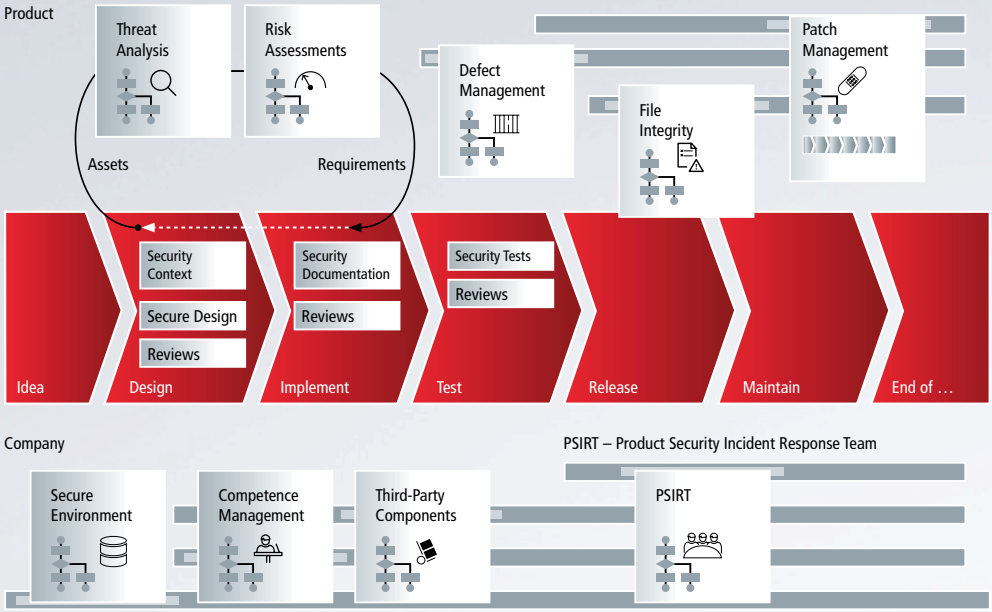
IT security best practices in view at an early stage

The early decision to implement TwinCAT on PC-based control systems with operating systems from the IT sector proved advantageous for IT security, because all functions originally developed for mass market IT systems were readily available for use with TwinCAT. Other control technologies with proprietary firmware, on the other hand, only started to develop security features in a holistic manner after the Stuxnet malicious computer worm was discovered.



Development lifecycle with IT security

Security functions can only be effective if they are planned for and deployed in a system efficiently. Beckhoff products provide a solution with continuously expanded security guides for IPCs, which now cover several operating system generations. In addition, a lifecycle has been established for these products, with IT security ensured from product conception to discontinuation. This lifecycle is continuously reviewed and improved. Security properties in products have been created along with other processes for the benefit of the user. Development tools from Beckhoff support engineers in related projects, e.g., through Source Control in TwinCAT Engineering (TE1000).

Product features include, for example:

- Encrypted protocol Secure ADS for communication between all instances of TwinCAT
- Communication protected via security protocols such as TLS for TwinCAT IoT Communication (TF6701)
- Mechanisms for intellectual property protection of source code and projects in engineering and at runtime via software protection
- Communication protected by the HTTPS protocol for TwinCAT HMI (TE2000)

In TwinCAT OPC UA (TF6100), almost all security functions of the associated standard are implemented as well.

These product features contribute to IT security, along with real-world processes in the entire supply chain. As a trusted supplier, Beckhoff regularly provides customers, for example, with information about operating system updates that have been tested for compatibility with TwinCAT 3, as well as a process for handling and publishing security vulnerabilities. Beckhoff established its own Product Security Incident Response Team (PSIRT) at an early stage, with secure communication channels to customers, security analysts and national and international bodies that coordinate the handling of security issues. The IT security platform CERT@VDE from VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V. (German Association for Electrical, Electronic & Information Technologies) was launched with the support of Beckhoff. Via this platform, small and medium-sized enterprises (SMEs) in the field of automation technology can receive support on IT security issues.

However, the TwinCAT philosophy is not only about functions and processes, but also about principles: During further development, existing and new default settings are designed in such a way that they are already "secure", following the principle of Secure by Default.

Torsten Förder,
Product Management
TwinCAT, Security

More information:
www.beckhoff.com/secguide
www.beckhoff.com/secinfo