emlix
embedded linux systems

Embedded Linux Security

As a consequence of Industry 4.0, the industrial internet and concerns over cyber security, manufacturers, integrators and operators of industrial products are facing an increasing number of new legal and market requirements. IT and system security and secure M2M communication have become important issues affecting competitiveness.

emlix offers adaptable system components that increase the system security of industrial embedded Linux systems. We also provide tools and processes to maintain the achieved security level over the entire product life cycle. The spectrum of emlix's security solutions ranges from networked systems with „industry-level basic protection" to high-security systems. The defined level of security needs to be cost-effective and scalable as well as readily maintainable.

Security components

When it comes to developing new products, adaptable security components are used as central, pre-configured building blocks for the quick and economical implementation of an appropriate system security concept.

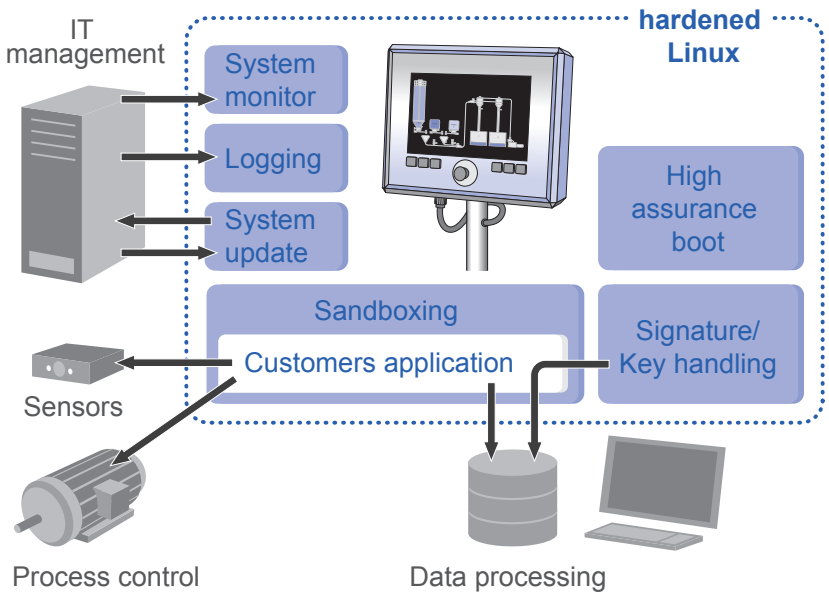
The use of mainline-based components not only ensures state-of-the-art technology. These sources also provide investment security and are easy to maintain: community-generated innovations and fixes can be directly adopted. The security components that emlix has frequently implemented include:

- Infrastructure for hardened Linux systems
- Secure booting for the integrity of Linux and of the application
- Sandbox environment to isolate applications
- Secure interprocess communication
- Encrypted system status diagnostics data
- Encrypted notification of events such as maintenance

Scalable security for industrial products

- Secured network connections
- Infrastructure for signed security patches
- Procedures to verify the integrity of updates
- Automated system integrity tests

We work in close collaboration with our customers to adapt these components to the specific requirements of each product and its application context.



emlix
embedded linux systems

Security Monitoring

emlix's security monitoring helps you maintain the defined security status of embedded Linux-based industrial products in the operating and maintenance phase.

We monitor relevant information sources as well as security findings (CVEs, Common Vulnerabilities and Exposures) and evaluate possible risks in light of the product-specific application context and the risk profile of your product. A security report provides you with specific recommendations for security patches and updates.

The IT security act demands security lifecycle management for industrial control systems (ICS). Security monitoring ensures the relevant processes.

The IT Security Act requires security life cycle management for industrial control systems (ICS). Our security monitoring ensures that this process takes place.

The objective is to identify relevant security fixes, new software versions and improvements to relevant components as soon as possible and then to check whether and when they should be integrated into the productive system (security patch management).

Our build automation system e2factory ensures that these changes are transparent and enables defined system security for board support packages.

emlix GmbH

solutions @ emlix.com
http://www.emlix.com

Phone +49 (0) 551 / 30664-0
Fax +49 (0) 551 / 30664-11

Security Review

We provide a sophisticated security review for the evaluation of system and network security for open-source-based industrial products. This includes running the necessary network tests and an analysis of the Linux software platform that is in use. The security review provides an analysis of the product's security status, indicates possible risks and offers clear suggestions.

Industrial products are increasingly tested for IT security by the operators. A security review helps identify and address security issues in advance.

Industrial control systems security is audited by risk assessments of the operating companies. Our security review helps to identify and close security holes in advance.

The security review follows industrial best practices. We want our customers' developers, product managers and marketing teams to be able to evaluate the current stage of development in light of customer requirements regarding „cyber security", „embedded IT compliance" and „industrial security".

An emlix security review includes the following services:

- Analysis of the product and of its application environment
- Execution of network and interface tests
- Analysis of the software packages in use and CVEs
- Evaluation of the software basis and architecture

The results of the review are summarized in a report together with specific recommendations for action. The process always concludes with an assessment of the risks and defensive measures in consultation with the customer's developers and product managers.