IGLOS – Industrial Grade Linux Operating System

Choosing the right platform is critical for industrial embedded systems. IGLOS is a secure embedded Linux distribution that is fully aligned with the Cyber Resilience Act. Unlike generic embedded Linux distributions, IGLOS combines certified processes, hardened security features and professional support to keep devices secure, compliant and future-ready. IGLOS offers open and proven Linux-based technologies and supports easy integration of third-party applications. Industrial robots, high-speed trains, edge cloud clusters, or any other system you can imagine – it can be built with IGLOS.

IGLOS by LINUTRONIX

Core Features

- Tailored to Your Use Case
- For ARM, Intel and Further Architectures
- Continuous Security Maintenance
- Full Secure Boot Chain
- Signed and Encrypted A/B Updates
- Integrity Protection for Software
- Encrypted Data at Rest and in Transit
- Hardened Linux
- Real-Time Support - by the Preempt-RT Team

Certified Security

With IGLOS Secure Beacon we provide a blueprint for all 57 applicable IEC 62443-4-2 security requirements and a fully traceable compliance documentation. With the independent certification by TÜV SÜD, the processes and implementations are proven to align with state-of-the-art security practices.

Industrial IT Security
TÜV SÜD
IACS Component
Secure Product Development Lifecycle assessed & monitored according to IEC 62443-4-1
Technical Security Requirements assessed according to IEC 62443-4-2

Secure Boot

IGLOS implements a secure boot mechanism to ensure integrity and authenticity already during boot. Our secure boot solution enforces verification of bootloaders, the Linux kernel and the full root file system. It prevents unauthorized or unsigned code from running during the boot process, protecting the system from boot-level malware and rootkits, as well as from injection of malicious software at runtime. This is the root of trust of all other security mechanisms built on top. To reliably sign new software images, even after critical security incidents, a stable central signing infrastructure, using a HSM and based on open source software, is available that you can easily deploy in your own environment.

Secure Update

Secure, encrypted atomic updates for the OS keep the devices secure. With IGLOS, devices can be updated regularly and in large batches by deployment services, ensuring they always have the latest security patches installed. These updates are extremely important for the operation and maintenance of the devices. If there is a problem with an update, the devices are rolled back to a stable state. This guarantees the functionality of a device at all times. Updates are also necessary to add new functionalities to a device in the field. The open-source software SWUpdate is used as the base for the update daemon on the devices. Alternative solutions like RAUC, Mender or Uptane are available upon request.

Defense in Depth

Layered and complementary security mechanisms are implemented throughout the entire embedded Linux stack to ensure that no single control is relied upon exclusively, enhancing the protection of systems using IGLOS. It implements mandatory access control (e.g., AppArmor) to restrict what programs can do, audit logging to detect and investigate suspicious activity, and a firewall to mitigate network-based attacks. Together with secure boot, secure update and encrypted application data and isolation of executable code from volatile data, these overlapping protections reduce the impact of individual failures or exploits. By implementing defense across boot, kernel, access controls, logging, and networking layers, IGLOS raises the bar for attackers and increases the chance that attacks are prevented or detected before causing serious harm.

Containers, VMs or Debian Packages

Using containers, applications - also from other parties - can be easily installed on the platform. Hereby an application with all its dependencies is bundled in one package. This simplifies the initial installation as well as regular updates. IGLOS uses Podman, a secure and Docker-compatible runtime for OCI containers. Alternatively, a hypervisor like Jailhouse can be used to deploy applications in virtual machines, instead or alongside to containers. Finally, Debian packages can be conveniently used for native deployment of custom software with minimal footprint as well.

Device Management

Systems based on IGLOS integrate seamlessly with established device management platforms such as Eclipse hawkBit, enabling automated software updates and fleet management. Operating systems and applications can be securely deployed and updated across individual devices or entire fleets, on-premise or in the cloud. With zero-touch onboarding, a fast, secure, and scalable provisioning at first power-up can be realized, protecting device identities and ensuring continuous delivery of the latest security patches.

Your Path with IGLOS

Escape the CRA Labyrinth with IGLOS

Linutronix GmbH
Bahnhofstraße 3 | D-88690 Uhldingen-Mühlhofen
Phone: +49 7556 25 999 0 | sales@linutronix.de
www.linutronix.de | Visit us

Are you interested?
Would you like to learn more about our products and solutions?
Simply contact us via phone or email.