EDGE Device
Security Paper

ENGEL
be the first

Technical safety

TPM

The EDGE Device has a TPM 2.0 chip built in. This is used for cryptographic operations such as storing keys. Among other things, it is also used for encrypting the SSD.

This way we can guarantee that the EDGE Device is not manipulated or data is not read out. If, for example, the SSD is replaced, the system will no longer boot up.

In addition, the EDGE Device locks itself after a certain number of attacks, which also prevents a possible attack.

Interfaces

When designing the EDGE Device, care was taken to minimise the number of hardware interfaces as much as possible. In addition, existing interfaces are severely limited. For example, the EDGE Device has a USB port, but no USB stick can be connected and used. Furthermore, the BIOS is encrypted and cannot be changed.

Applications

Only the most important services, such as the update mechanism of the EDGE Device, run as components directly on the Debian operating system. All other applications run as microservices in secure Docker containers. The individual Docker containers are only started if the services running in them are actually needed. In addition, only containers that have been explicitly accepted, tested and signed by ENGEL can be loaded onto the EDGE Device. Details on the checks of the services in the Docker Containers can be found in the chapter “Dependency Check”.

By using Docker, we can ensure that a possibly infected or taken-over container nevertheless does not have access to the operating system or other containers. There are limited defined APIs for communication between containers.

Access to the EDGE Device

There is no user on the EDGE Device who can log on to bash, for example. Thus, the operating system of the EDGE Device cannot be accessed directly

locally. The EDGE Device can be configured with an IP address and onboarded via a web wizard, which is only directly available on the LAN interface SUPPORT. All other access to the EDGE Device is via clients serving a specific purchased ENGEL service. These clients in turn do not have full access to the EDGE Device but run in a Docker container.

The configuration of the EDGE Device (with the exception of the network configuration) can therefore only be carried out remotely, e.g. in the ENGEL customer portal. For this purpose, the EDGE Device requires a connection to the ENGEL endpoints. This in turn allows us to ensure that only a genuine ENGEL EDGE Device receives updates and configurations from ENGEL.

EDGE Device Connection to ENGEL

When the EDGE Device is installed by our manufacturer, each EDGE Device is provided with a unique hardware certificate.

In order for the EDGE Device to establish a connection to the ENGEL endpoints, it must be initially on-boarded once. To do this, a token must be requested in the customer portal for the EDGE Device received using the combination of serial number and the test number that is affixed to the EDGE Device. This token must then be entered in the web assistant, which can only be reached via the LAN interface SUPPORT on the EDGE Device, after the configuration of the IP address and is only valid for an onboarding of this one device. Immediately upon entry, the EDGE Device attempts to establish a connection to e3.engelglobal.com on port 443. The server checks whether the combination of hardware certificate and token matches. This mechanism checks that the EDGE Device has not been manipulated or exchanged during dispatch from the supplier to the customer.

If the combination of hardware certificate and token matches, the EDGE Device receives a client certificate that is used for future communication. For this reason, no packet inspection may be performed for the communication of the EDGE Device to the ENGEL endpoints. If a packet inspection is performed, the e3.engelglobal.com will not accept the connection of the EDGE Device.

If the EDGE Device is unable to connect to e3.engelglobal.com for several months, the client certificate expires and the onboarding of the EDGE Device must be performed again.

The EDGE Device does not establish standing connections but, depending on the application, either relies on polling or regularly renews the connections. This ensures that no key is used for too long.

Process safety

Safety before hardware replacement

The EDGE Device is installed directly by the hardware supplier. The EDGE Device also receives a unique hardware certificate, which is stored on the EDGE Device. In addition, this hardware certificate is stored at ENGEL so that a comparison can be made later.

When onboarding the EDGE Device in the customer portal, the checksum, which is affixed to the device, must be entered in addition to the existing EDGE Device serial number. By entering the checksum, you receive a token that is only valid for this one EDGE Device for a successful onboarding.

The token must then be entered in the web assistant of the EDGE Device after configuring the IP address. Directly upon entry, the EDGE Device attempts to establish a connection to e3.engelglobal.com. The e3 server checks whether the combination of the hardware certificate with the token is valid. If this is the case, the EDGE Device is issued a client certificate for further communication. This client certificate is renewed automatically on a regular basis if the EDGE Device can establish a connection to the ENGEL endpoints.

By using the TPM chip and SSD encryption, we can ensure that the EDGE Device has not been cloned or tampered with. By using the hardware certificate together with the onboarding process, we can also exclude the possibility of an attacker impersonating an EDGE Device or attempting to replicate an EDGE Device.

Updates

Updates can only be carried out remotely. For this, the EDGE Device needs a connection to e3.engelglobal.com. Via this mechanism, the EDGE Device can obtain any kind of updates (operating system, components, Docker containers, etc.). However, the EDGE Device only receives updates that have been tested and approved by ENGEL.

Operating system and components

Updates for the Debian operating system and components are carried out regularly. Major upgrades are also carried out remotely. All updates are tested and checked several times at ENGEL before they are rolled out in waves to all EDGE Devices.

Docker Container

As with the operating system, there are regular updates for the services that run as Docker containers. These updates are also checked and tested in waves at ENGEL before being rolled out. Before a new version of a Docker Container is rolled out, it must be signed. The EDGE Device can only download and launch signed containers. This allows us to ensure that no containers are started on the EDGE Device that have not been approved by ENGEL.

Security in the development process

Dependency Check

In order to be able to react as quickly as possible to any vulnerabilities that arise, we use automated dependency checks in our development process. We distinguish between self-developed software and delivered software. Delivered software is, for example, the Debian operating system or services (Docker containers) of applications that have been purchased, such as e-connect.24.

If a dependency with a vulnerability is discovered in the production system, the affected software is updated. The time period of the update depends on the CVS of the vulnerability.

Self-developed software

For all software developed by ENGEL and running on the EDGE Device, a dependency check is carried out in the pipeline. This means that we can guarantee that no software is delivered with a known vulnerability at the time of delivery.

To ensure that productive software is not only tested when adjustments are made, but on a regular basis, this pipeline runs through weekly.

Software supplied

In order to also check the operating system and purchased Docker containers for possible vulnerabilities with the dependency check, there are two EDGE Devices in our test setup on which all Docker containers are running that ENGEL has in use. One EDGE Device represents the current productive state and one device represents the development state. These devices are now completely scanned weekly by a central ENGEL IT service and checked for possible dependencies with known vulnerabilities. In the process, both the operating system with all components and the running Docker containers are checked.

Penetration test

At regular intervals, a penetration test is carried out by an independent company for the EDGE Device and the ENGEL endpoint. The results are then incorporated into the development of the EDGE Device.