Documentation - Security on EOR-3D

Version: 1.5

Creation Date: 2019-11-29
Release Date:

Author	Department	Changes	Version	Date
Security developer	-	Initial Version	1.0	2018-07-04
Security developer	-	Added default PIN	1.1	2019-07-02
Security developer	-	changes description	1.2	2019-08-13
Security developer	-	changes description	1.3	2019-09-11
Security developer	-	changes description	1.4	2019-11-14
Security developer	-	Change bootloader	1.5	2019-11-29

Distribution:

Name	Department	Location	Version

Table of Contents

1 Document description

This document describes the security features and concept of the EOR-3D device.

2 TCP/UDP ports and services on an EOR-3D

UDP Port 45454 – UDP Toolbox search – general always insecure, simple UDP search on the Network

TCP Port 3002 – TCP Toolbox connection – insecure and secure
TCP Port 3005 – GUI Toolbox connections – insecure and secure
TCP Port 20/21 – FTP and FTPS – insecure and secure

TCP Port 22 – SSH – secure with cryptographic password

TCP Port 5900 – VNC – insecure
TCP Port 2404 – T104 – insecure
TCP Port 502 – Modbus – insecure
TCP Port 20000 – DNP30 – insecure

3 Security concept

The EOR-3D security concept includes cryptographic connections on all ports and services for communication. SCADA connections without cryptographic can be switched of by the firewall.
A TLSv1.2 connection with RSA Certificate and symmetrical encryption with Elliptic Curves Certificates is used for Toolbox connection.

A Firewall is included which does check for port scans and blocks all other possible connections.
Different users levels can be used to allow different user roles. Passwords are controlled over private certificates from A-Eberle.

3.1 Secure TCP connection

`E3D_sec_mode=1` is default and can not switched off, following communications are encrypted:

TCP Port 3002 – Toolbox connection commands will run as TLSv1.2 with AES encryption inside the TLS channel
TCP Port 3005 – Toolbox GUI will run with AES encryption.
TCP Port 21 and FTP/FTPS passive ports - FTP runs as FTPS

3.2 Security parameters

Security parameters are divided from standard parameters, they are only accessible if the Userlevel has Admin rights.

3.2.1 Security parameters – User Handling

```
E3D_panel_users_active=0
E3D_tcp_users_active=0
E3D_ro_pin_active=0
E3D_rw_pin_active=0
```

3.2.2 Security parameters – Firewall

```
E3D_Firewall_dis=0

E3D_FW_ETH0_com=1
E3D_FW_ETH0_ssh=1
E3D_FW_ETH0_vnc=1
E3D_FW_ETH0_mod=1
E3D_FW_ETH0_104=1
E3D_FW_ETH0_DNP3=1
E3D_FW_ETH0_ACT=0

E3D_FW_ETH1_com=0
E3D_FW_ETH1_ssh=0
E3D_FW_ETH1_vnc=0
E3D_FW_ETH1_mod=1
E3D_FW_ETH1_104=1
E3D_FW_ETH1_DNP3=1
E3D_FW_ETH1_ACT=0

E3D_FW_ETHW_com=0
E3D_FW_ETHW_ssh=0
E3D_FW_ETHW_vnc=0
E3D_FW_ETHW_mod=0
E3D_FW_ETHW_104=0
E3D_FW_ETHW_DNP3=0
E3D_FW_ETHW_ACT=0

E3D_FW_BLOCK=3600
```

All open UDP/TCP ports can be controlled by the firewall and switched “ON” or “OFF” with the Toolbox.

WARNING: On change of firewall parameters the device has to be rebooted!

3.2.3 Security parameters – FTP/FTPS

```
E3D_ftp_pasv_pro=0
E3D_ftp_min_passive=1024
E3D_ftp_max_passive=1124
```

WARNING: On change of FTP/FTPS parameters the device has to be rebooted!

3.2.4 Security parameters – BOOTLOADER

```
E3D_Disable_boot_timeout=0
```

To disable the Bootloader delay, this parameter has to be set to 1.

WARNING: On change of Bootloader parameters the device has to be rebooted!

3.3 User handling

The user handling can be controlled with:

- `E3D_panel_users_active`
- `E3D_tcp_users_active`

`E3D_panel_users_active` is for panel GUI users.
`E3D_tcp_users_active` is for TCP users.

3.3.1 User handling – Panel GUI

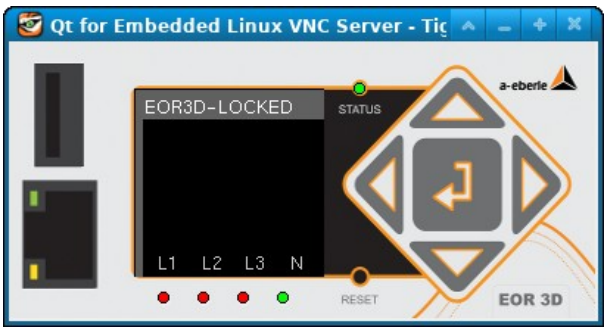
If `E3D_panel_users_active` is active, there a two possible default users. A user with user rights and have read only access and a user with operator rights with read and write rights.
These two default users can be controlled with the parameters:

- `E3D_ro_pin_active`
- `E3D_rw_pin_active`

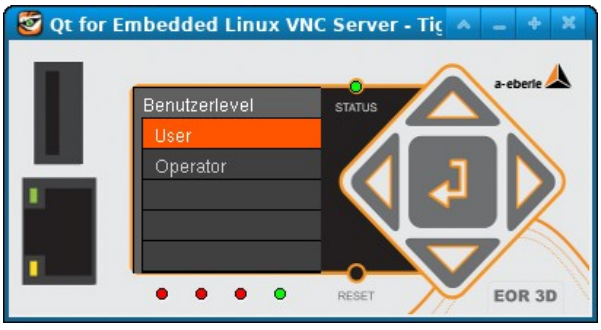
If both are inactive and `E3D_panel_users_active` is active, the GUI panel is locked!

3.3.2 User handling – Panel GUI – example configurations

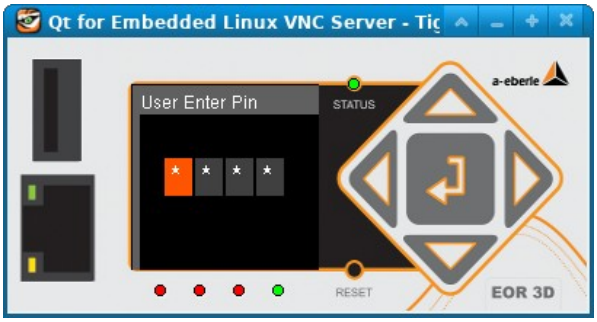
- `E3D_panel_users_active=1`
- `E3D_ro_pin_active=0`
- `E3D_rw_pin_active=0`



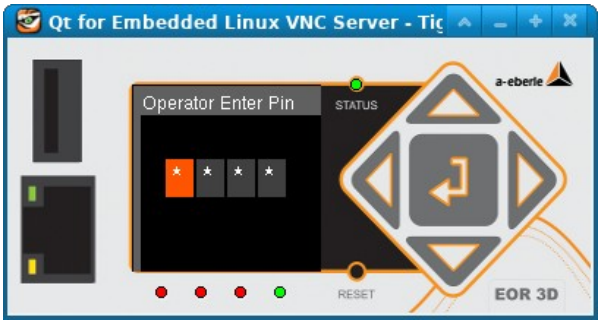
- `E3D_panel_users_active=1`
- `E3D_ro_pin_active=1`
- `E3D_rw_pin_active=1`



- E3D_panel_users_active=1
- E3D_ro_pin_active=1
- E3D_rw_pin_active=0



- E3D_panel_users_active=1
- E3D_ro_pin_active=0
- E3D_rw_pin_active=1



3.3.3 User handling – TCP

If E3D_tcp_users_active is active the user handling take place.
With the Toolbox a login with username an password has to be done.

3.3.3.1 User handling – TCP – User Groups

Several users can be added to this groups with the Toolbox. Following user groups are possible:

- User → Users in this group have read only access
- Operator → Users in this group have read and write access
- Admin → Users in this group have read and write access and can change security parameters

3.3.4 PIN / Passwords / standard passwords

Pins and Passwords are stored in the standard Linux password database on the device.

Standard passwords(root and ftp), also without security are changed to secure passwords!
A FTP login without a password is not allowed.

3.4 Cryptographic keys / Certificates

The EOR-3D device generates on the first start up two self signed certificates!

The Toolbox command channel with TLSv1.2 and FTPS with TLSv1.2 connection uses a RSA 2048 bit Certificate at /appfs/eor3dapp1/eor3d.pem.

Inside the TLSv1.2 Toolbox command channel and for the Toolbox GUI channel a symmetrical encryption with an elliptic curves Certificates with 512bit at /appfs/eor3dapp1/eor3d_ec.pem is used (ecdsa-with-SHA256).

3.5 Cryptographic keys / Certificates for password generation

These are close and only known by A-Eberle for ftp users and SSH root user.