Pump Firmware Update

1. Introduction

1.1 Purpose

This document outlines the software requirements for the **firmware update process** of the cooling unit pump. The goal is to ensure seamless, secure, and reliable firmware upgrades, improving performance, security, and bug fixes without disrupting operations.

1.2 Scope

The firmware update software will:

- Support **local firmware updates**.
- Ensure a **fail-safe** update process.
- Provide **real-time status monitoring**.
- Be compatible with **AROS pump models** used in cooling systems.

2. Functional Requirements

2.1 Firmware Update Mechanisms

- ~~**Remote Update:** Via **Ethernet, Wi-Fi, or IoT gateway** (e.g., MQTT, Modbus TCP/IP).~~
- CIOC board can be updated via USB stick or ethernet (FTP/SFTP/Web). In case the update contains a pump firmware update, then the CIOC updates the pumps via CAN bus.
- **Local Update:** Via **direct serial connection (CAN bus)**.
- ~~**Over-the-Air (OTA) Update:** If applicable, updates should be deployable over a network securely.~~

2.2 Update Process Flow

1. **Search for updates**

   In the following scenarios the CIOC searches for new firmware updates:

   - Automatically after every bootup of the CIOC
   - Manually after exchange of a CCU in service cases

~~1.~~2. **Firmware Verification**

   - Check **firmware integrity** before installation using check sum embedded in the firmware.
   - ~~Verify compatibility with the pump model.~~

~~2.~~3. **Pre-Update Safety Checks**

Commented [PP1]: Check with Bjoern if both can be possible?

Commented [BH2R1]: We support only local update. So after each bootup of the pump. Or do you mean cioc updates ? This could be done by network

Commented [PP3R1]: Freeze for Local firmware update (Pump update is a part of CIOC update)

Commented [PP4]: Is it already implement?

Commented [BH5R4]: What do you mean with fail- safe ? We try it 3 times, after that we give up.

Commented [PP6R4]: Only include fail safe update process

Commented [PP7]: Can be provided? Or is it already there?

Commented [BH8R7]: We only do a matchgrade. So the software what is installed in the cioc board, will flashed to the pump

Commented [PP9R7]: Already there and no option for roll back

Commented [PP10]: Do we have multiple pump models?

Commented [BH11R10]: Yes, if they all have the same software

Commented [PP12R10]: Be Compatible with AROS pump model (Get pump model name from hardware team)

Commented [PP13]: What all in our scope?

Commented [BH14R13]: We can use a USB Stick or ...

Commented [BH15R13]: CIOC Update with WEB or U ...

Commented [PP16R13]: Not in the scope

Formatted: Font: Not Bold

Commented [PP17]: Only CAN bus support is there

Commented [PP18]: For future with NFC. Needs more ...

Commented [BH19R18]: NFC is to slow, we need ...

Commented [PP20R18]: Not in the scope

Commented [PP21]: Bjoern to confirm if we've similar ...

Commented [BH22R21]: The pump software don't us ...

Formatted: Font: Bold

Formatted ...

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Commented [PP23]: Check Firmware integrity before ...

Commented [PP24]: Not in the scope as of now

- ~~Ensure the pump is in a safe state before updating (e.g., idle or standby mode).~~
- Notify users if the system needs to be paused.
- Firmware update for the pumps must be agreed by the customer in a dialog.

3.4. **Firmware Installation**

- Write new firmware to the microcontroller/ECU flash memory.
- Ensure atomic updates to prevent partial firmware corruption.

4.5. **Post-Update Verification**

- ~~Perform a self-check to confirm firmware integrity.~~
- Restart the pump and validate normal operation.

5.6. **Rollback Mechanism** (Failsafe)

- ~~If the update fails, automatically revert to the **last known working firmware**.~~
- Log the failure for diagnostics.
- In case the update has failed 3 times for a pump, there has to be an alarm message, to inform the user that the pump is not going to work. All other pumps where update was successfully completed have to switch back to their normal operation in automatic mode.

2.3 User Interface for Updates

- **WebUI:** Show update progress (e.g., percentage completed, estimated time).
- **Notifications:** Alert users about updates via **email**.
- **Logs & Reports:** Maintain a log of update history, and errors.

2.4 Security Measures

- Firmware shall comply with IEC 62443-4-2
- **Signed Firmware Packages:** Use **digital signatures** to prevent unauthorized updates.
- ~~**Authentication:** Require admin-level access for updates.~~
- **Encryption**: Secure firmware files in transit and storage using **AES-256**. It shall support TLS and SSL authentication and encryption.

~~2.5 Compatibility & Integration~~

- ~~**Supported Pumps:** Ensure compatibility with different pump models.~~
- ~~**Communication Protocols:** Support **Modbus, BACnet, MQTT, HTTP/HTTPS, FTP** for remote updates.~~
- ~~**SCADA/BMS Integration:** Allow remote monitoring of firmware status via API.~~

Commented [BH25]: After Bootup we update the pumps so there should not be a regulation

Commented [PP26R25]: Not in the scope

Commented [BH27]: We only show the update status in the web

Commented [PP28R27]: Keep it open for future discussion

Commented [BH29]: Yes, one after another

Commented [PP30R29]: It will try for 3 times

Commented [BH31]: We don't have a self check, we have to ask concentrics what they do

Commented [PP32R31]: Not in the scope for now

Commented [BH33]: After each updatge, the pump is rebootet

Commented [PP34R33]: Just check the status of the pump

Commented [BH35]: No, there is no second partition on the pump. If the update fails, we try it 3 thimes, after that the pumps is dead

Commented [PP36R35]: Not possible as of now

Commented [BH37]: We log that a update has started, finished or an error

Commented [PP38R37]: Already implemented

Commented [BH39]: We don't have an HMI Display, we only have the Web Interface

Commented [BH40]: SMS not possible, Email must be configured by the customer

Commented [BH41]: We only use the Log File for CIOC but without versions

Commented [PP42R41]: For customers firmware version is not important to show

Commented [CR43R41]: You mean the firmware version of the pumps, right?

Formatted: Font: Not Bold

Commented [BH44]: So far as i know. there is no signature.

Commented [PP45R44]: Discuss it with Christine and Barbel

Commented [CR46R44]: Is it required to comply with IEC 62443-4-2?

Commented [BH47]: For the Bootup we don't need admin rights, i think we have to differ between the cioc ...

Commented [PP48R47]: Not in the scope

Commented [PP49]: Check with Barbel and Christine

Commented [CR50R49]: Is AES-256 part of a TLS/ SSL ...

Commented [PP51]: Not required remove

3. Non-Functional Requirements

3.1 Performance

- **Firmware update time:** **<1 minute 10 secs** per pump for a typical update (~385KB firmware).
- **System downtime:** Should be **<1 minute** after the update completes.

3.2 Reliability

- Ensure **99.9% update success rate** with rollback in case of failures.

3.3 Scalability

- Support firmware updates for **pumps one after another at a time,** all other pumps are set to 80% while the update is in-progress

~~3.4 Security~~

- ~~Ensure **role-based access control (RBAC)** for firmware management.~~

~~4. Error Codes & Troubleshooting~~

~~Code~~	~~Error Description~~	~~Action~~
~~FW001~~	~~Firmware file not found~~	~~Check file path or URL.~~
~~FW002~~	~~Firmware signature mismatch~~	~~Verify firmware authenticity.~~
~~FW003~~	~~Update failed – low power~~	~~Ensure stable power source.~~
~~FW004~~	~~Communication timeout~~	~~Check network or USB connection.~~
~~FW005~~	~~Rollback activated~~	~~Investigate previous firmware issue.~~

---

5. User Interface Requirements

~~5.1 HMI / Web Dashboard~~

- ~~**Firmware Update Tab** with:~~
  - ~~**Upload** button for local updates.~~
  - ~~**Check for Updates** option for remote updates.~~
  - ~~**Progress Bar** to show update status.~~
  - ~~**Logs Section** to view past firmware versions.~~

~~5.2 Mobile/Remote Monitoring~~

- ~~Receive **push notifications** on firmware update success or failure.~~

Commented [PP52]: Check with Bjoern what's the best and worst case window for this?

Commented [PP53R52]: 70 Secs per pump (385 KB firmware)

Commented [PP54R52]: Also need to check during testing

Commented [PP55]: Check with Bjoern what will be the down time in worst case. Can also be evaluated in stress testing.

Commented [PP56R55]: 21 mins best case

Commented [CR57R55]: Is there a system downtime if each pump is updated after the other?

Commented [CR58R55]: During update of CIOC for approx. 2min, the pumps run in fail safe mode

Commented [CR59]: ALL other pumps, means 14 or 11 pumps?

Commented [PP60]: Not there we don't need this

Commented [PP61]: Check with Bjoern do we have similar sort of error codes?

Commented [PP62R61]: Not required

Commented [PP63]: Not required

Commented [PP64]: Not required

6. Testing Requirements

6.1 Functional Testing

- Validate update process under **normal and edge cases** (e.g., power loss during update).

~~6.2 Security Testing~~

- ~~Ensure firmware files cannot be **tampered with or replaced by unauthorized files**.~~

6.3 Performance Testing

- Test update speed over **different network conditions (Wi-Fi, Ethernet, 4G/5G, satellite IoT)**.

7. Maintenance & Support

7.1 Firmware Versioning

- Use **semantic versioning** (e.g., v1.2.3) to track updates.

7.2 Documentation

- Provide detailed **firmware release notes and update procedures**.

7.3 Support

- Offer **remote troubleshooting and rollback assistance** in case of failures.

Commented [PP65]: Not required

Commented [PP66]: Not required but also check with other people

Commented [PP67]: Only with Ethernet

Commented [PP68]: Keep it open for discussion