Software Requirements Specification (SRS) for Fail Safe Mode

System Name: Direct Liquid Cooling (DLC) In-Row

Module: Fail Safe Mode

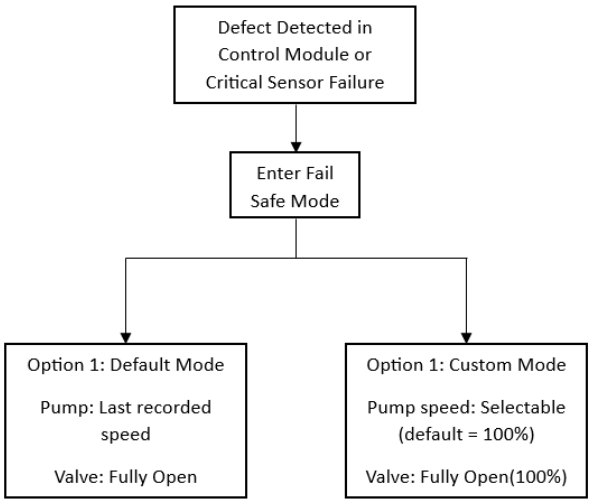
Version: 1.0

Date: June 06, 2025

Author: Prateek Bawane

1. Introduction

Fail Safe Mode



1.1 Purpose

This document outlines the software requirements for implementing the **Fail Safe Mode** in the CDU to ensure continued coolant flow and system protection in the event of a control module or critical sensor failure.

1.2 Scope

Applicable to the CDU control software managing pump and control valve behavior under fault conditions. Ensures continued coolant circulation during a failure scenario to protect the connected infrastructure.

---

2. Definitions and Abbreviations

- **CDU:** Coolant Distribution Unit.
- **Fail-Safe Mode:** A predefined operational mode in which the CDU continues functioning safely during a critical failure.
- **Control Valve:** A modulating valve used to control liquid flow.
- **Pump Speed:** The RPM or percentage speed of the CDU pump.
- **Default Mode:** The standard pre-configuration behavior of the CDU during fail-safe mode.

---

3. Functional Requirements

Requirement ID	Requirement Description	Priority	Default
FR001	System shall detect a defect in the control module or critical sensor (Secondary supply pressure sensor(P1), secondary return pressure sensor(P2), secondary supply temperature sensor(T1)).	High	-
FR002	Upon detection of a failure, system shall automatically transition to **Fail-Safe Mode.**	High	Yes
FR003	Fail-Safe Mode shall have two selectable options configured by the user.	Medium	Option 1
FR004	In Option1 (Default Mode): Pumps shall run at the last	High	Yes

Commented [CR1]: How about interruptions of the CAN connection or communication?

Commented [PP2R1]: Yes that need to be considered as well

	recorded speed, and the valve shall fully open.		
FR005	In option 2 (Custom Mode): Pumps shall run at a selectable speed (default = 100%), and the valve shall fully open (100%).	Medium	Configurable
FR006	The selectable Fail-Safe Mode option shall be configurable via HMI or setup interface,	Medium	Yes
FR008	Fail-Safe configuration shall be retained in non-volatile memory.	Medium	Yes
FR009	A log event shall be created upon entry into Fail-Safe Mode with timestamp.	Low	Yes
FR010	After the error has been rectified, the CDU automatically returns to the previous operating mode	High	Yes

Commented [CR3]: Does this mean the memory in the pumps?

Commented [PP4R3]: No in the CIOC board

Formatted: English (United States)

Formatted: English (United States)

Formatted: English (United States)

Formatted: English (United States)

4. Non-Functional Requirements

Requirement ID	Requirement Description	Priority
NFR001	Fail-Safe Mode transition time shall not exceed 2 seconds after defect detection.	High
NFR002	User configuration must persist after power cycle.	High
NFR003	Fault event and Fail-Safe Mode activation and de-	Medium

	activation must be logged in system diagnostic	