Template

Failure Protection Decision

software requirement & Design Spec.

失效保護策略

軟體需求及設計規格

fpd-srds

Version-00.01

|  |  |  |  |
| --- | --- | --- | --- |
| **Authors** | Fenix Tsai | **Date** | 2022/08/10 |
| Contributors | Fenix Tsai | **Date** |  |
| Approved | *DRAFT* | **Date** |  |

校訂記錄

|  |  |  |  |
| --- | --- | --- | --- |
| **REVISION** | **DATE** | **AUTHOR** | **SECTIONS/PAGES AFFECTED** |
| **REMARKS** | | |
| 00.00 | 2022.07.25 | Fenix Tsai |  |
| 初版 – 格式確立 | | |
|  |  |  |  |
|  | | |
|  |  |  |  |
|  | | |
|  |  |  |  |
|  | | |
|  |  |  |  |
|  | | |
|  |  |  |  |
|  | | |
|  |  |  |  |
|  | | |
|  |  |  |  |
|  | | |
|  |  |  |  |
|  | | |
|  |  |  |  |
|  | | |
|  |  |  |  |
|  | | |
|  |  |  |  |
|  | | |

目錄

[1 簡介 4](#_Toc111032612)

[1.1 說明 4](#_Toc111032613)

[1.2 閱讀權限 4](#_Toc111032614)

[1.3 縮寫／術語定義 4](#_Toc111032615)

[1.3.1 縮寫定義 4](#_Toc111032616)

[1.3.2 名詞定義 4](#_Toc111032617)

[1.4 編號格式原則 5](#_Toc111032618)

[1.5 參考文獻 5](#_Toc111032619)

[2 模組功能需求 6](#_Toc111032620)

[2.1 模組功能彙整 6](#_Toc111032621)

[3 模組需求及邏輯設計 7](#_Toc111032622)

[3.1 ADCU\_SRDS\_01 系統故障策略解析 7](#_Toc111032623)

[3.1.1 ADCU\_SRDS\_01\_001 系統保護策略解析 7](#_Toc111032624)

[3.1.2 ADCU\_SRDS\_01\_002 系統故障警示燈策略 9](#_Toc111032625)

[3.2 ADCU\_SRDS\_01 系統故障策略解析 10](#_Toc111032626)

[3.2.1 ADCU\_SRDS\_02\_001 系統跛行模式判斷 11](#_Toc111032627)

[Appendix A 13](#_Toc111032628)

# 簡介

## 說明

此文件為ADCU的軟體需求及設計規格文件。主要是依據軟體需求矩陣文件Software Requirement Matrix(SWRM)、軟體的架構及Interface文件中提出所需的輸入輸出訊號，來彙整此模組功能需求，並依據需求來設計適當的軟體邏輯來對應。

## 閱讀權限

本文僅供 CubTEK跟**合作公司名稱** 內部的工程人員和管理人員使用。未經另一方書面許可，不得在這些組織之外散佈。

## 縮寫／術語定義

### 縮寫定義

|  |  |
| --- | --- |
| **名詞** | **描述** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

### 名詞定義

1. XXX：TBD

## 編號格式原則

本文中將需求及設計定義成一種編號，這些ID應具有唯一性，此 ID由固定字串和數字組成：

**軟體需求ID**：ADCU\_SRDS\_XX\_YY

XX：功能需求第一階層編號

YY：功能需求第二階層編號

## 參考文獻

1. FMVSS 111
2. Euro NCAP Test Protocol- AEB systems (most current)
3. Euro NCAP Test Protocol- AEB VRU systems (most current)
4. Euro NCAP Test Protocol- Lane Support Systems (most current)
5. ISO 26262
6. ISO 16750 1-5

# 模組功能需求

此章節說明由SWRM文件中所分析出用於FPD模組的功能需求

## 模組功能彙整

Table xx-xx FPD功能需求表

|  |  |
| --- | --- |
| SWRM編號 | 需求描述 |
| ADCU\_SWRM\_001 | 依據系統保護條件，判斷頗行模式  1. 正常模式：無任何異常。  2. 警示模式：關閉再生煞車或關閉DC充電或關閉AC充電或充電功率限制。  3. 動力限制模式：驅動動力限制或關閉DCDC或關閉TMS。  4. 無動力模式：關閉MCU。  5. 危險模式：關閉BMS。 |
| ADCU\_SWRM\_002 | 依據DDM模組判斷結果，發送警示燈需求給儀表  1. 整車系統異常警示燈需求  2. 電機過溫警示燈需求  3. 電機異常警示燈需求  4. 高壓電池過溫警示燈  5. 高壓電池異常警示燈需求  6. 低壓電源異常警示燈需求  7. 動力系統冷卻水過溫警示燈  當故障解除後，需維持系統保護，待重新開機後再依據最新狀態判斷是否成立。 |
|  |  |
|  |  |
|  |  |
|  |  |

# 模組需求及邏輯設計

此章節描述該模組之詳細功能需求描述，並依據描述設計邏輯及軟體搭建方式



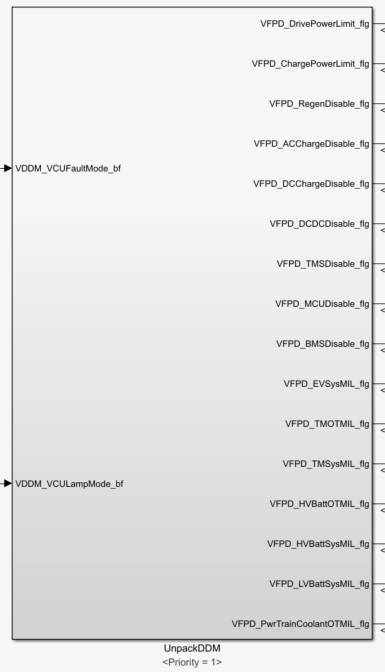
Figure XX-XX： 模組架構圖

## ADCU\_SRDS\_01 系統故障策略解析

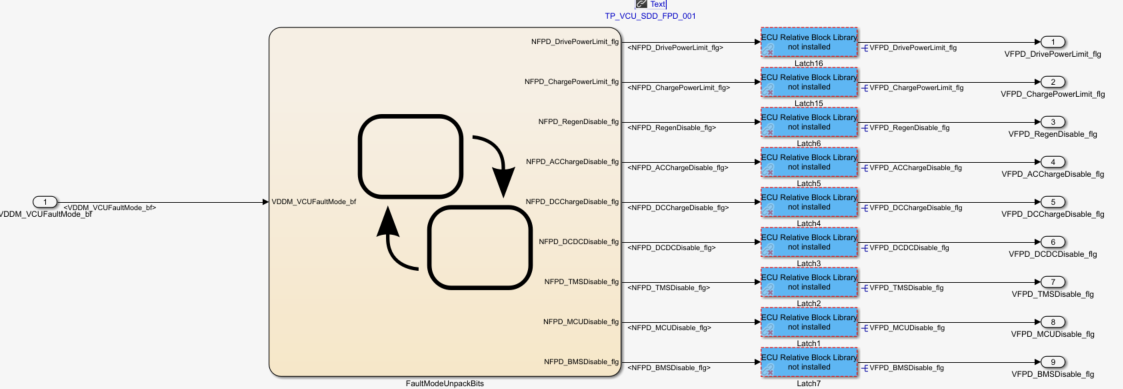
子功能架構圖

### ADCU\_SRDS\_01\_001 系統保護策略解析

依據DDM模組的故障管理資訊，將相關系統關閉保護並進入不同的頗行模式，使車輛能在安全的狀態下運行。



1. 依據DDM模組的故障管理資訊，將相關系統關閉保護並進入不同的頗行模式，使車輛能在安全的狀態下運行。設計如下：



將VDDM\_VCUFaultMode\_bf進行bit分析，每個bit代表不同的狀態，整車系統再依各狀態關閉相關功能。

FPD\_DrivePowerLimit\_flg = (VDDM\_VCUFaultMode\_bf & 0x01)。

VFPD\_ChargePowerLimit\_flg = (VDDM\_VCUFaultMode\_bf & 0x02) >> 1。

VFPD\_ACChargeDisable\_flg = (VDDM\_VCUFaultMode\_bf & 0x04) >> 2。

VFPD\_DCChargeDisable\_flg = (VDDM\_VCUFaultMode\_bf & 0x08) >> 3。

VFPD\_RegenDisable\_flg = (VDDM\_VCUFaultMode\_bf & 0x10) >> 4。

VFPD\_DCDCDisable\_flg = (VDDM\_VCUFaultMode\_bf & 0x20) >> 5。

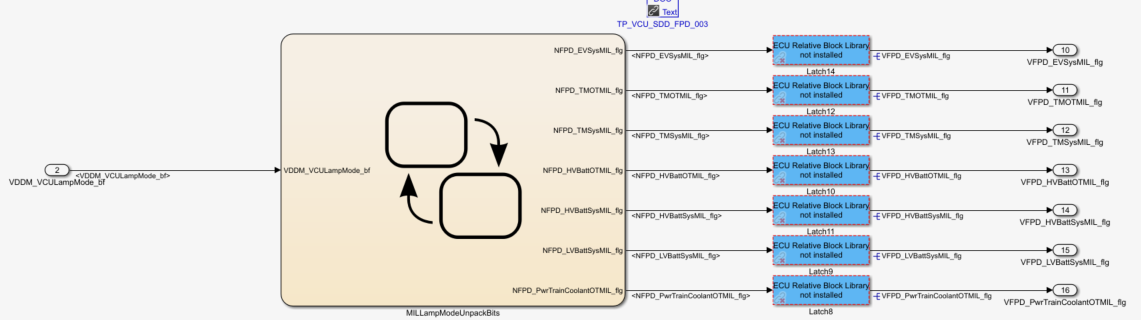
VFPD\_TMSDisable\_flg = (VDDM\_VCUFaultMode\_bf & 0x40) >> 6。

VFPD\_MCUDisable\_flg = (VDDM\_VCUFaultMode\_bf & 0x80) >> 7。

VFPD\_BMSDisable\_flg = (VDDM\_VCUFaultMode\_bf & 0x100) >> 8。

### ADCU\_SRDS\_01\_002 系統故障警示燈策略

依據DDM模組的警示燈管理資訊，控制相關警示燈提醒駕駛者注意。



將VDDM\_VCUFaultMode\_bf進行bit分析，每個bit代表不同的燈號需求，各燈號需求透過CAN發送給儀表顯示相關燈號。

VFPD\_EVSysMIL\_flg = (VDDM\_VCULampMode\_bf & 0x01)。

VFPD\_TMOTMIL\_flg = (VDDM\_VCULampMode\_bf & 0x02) >> 1。

VFPD\_TMSysMIL\_flg = (VDDM\_VCULampMode\_bf & 0x04) >> 2。

VFPD\_HVBattOTMIL\_flg = (VDDM\_VCULampMode\_bf & 0x08) >> 3。

VFPD\_HVBattSysMIL\_flg = (VDDM\_VCULampMode\_bf & 0x10) >> 4。

VFPD\_LVBattSysMIL\_flg = (VDDM\_VCULampMode\_bf & 0x20) >> 5。

VFPD\_PwrTrainCoolantOTMIL\_flg = (VDDM\_VCULampMode\_bf & 0x40) >> 6。

依據DDM模組的故障管理資訊，將相關系統關閉保護並進入不同的頗行模式，使車輛能在安全的狀態下運行。

車輛頗行模式主為分成正常模式、警示模式、動力限制模式、無動力模式及危害模式，各操作模式的定義如下：

正常模式(NORMAL)： 車輛無任何異常及故障。

警示模式(WARNING)：車輛診斷有異常或故障，但不影響車輛正常行駛。

動力限制模式(POWERLIMIT)： 車輛診斷有異常或故障，，但是輸出的功率會受到限制。

無動力模式(NOPOWER)：偵測元件異常，元件無法正常運作，關閉元件後，車輛無驅動力 (針對驅動電機異常)。

危害模式(HAZARD)： 偵測到元件異常或系統異常，需要緊急關閉高壓電迴路。

當故障條件成立後，若故障解除需維持故障保護狀態，待關機休眠後重新啟動才可解除。

## ADCU\_SRDS\_01 系統故障策略解析

車輛頗行模式主為分成正常模式、警示模式、動力限制模式、無動力模式及危害模式，各操作模式的定義如下：

正常模式(NORMAL)： 車輛無任何異常及故障。

警示模式(WARNING)：車輛診斷有異常或故障，但不影響車輛正常行駛。

動力限制模式(POWERLIMIT)： 車輛診斷有異常或故障，，但是輸出的功率會受到限制。

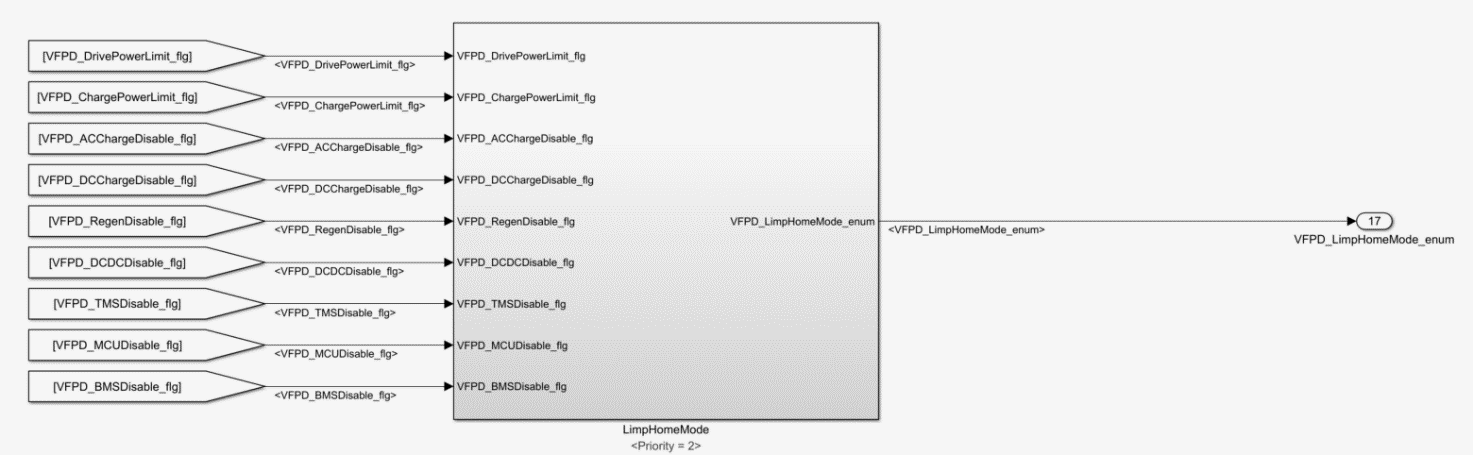
無動力模式(NOPOWER)：偵測元件異常，元件無法正常運作，關閉元件後，車輛無驅動力 (針對驅動電機異常)。

危害模式(HAZARD)： 偵測到元件異常或系統異常，需要緊急關閉高壓電迴路。

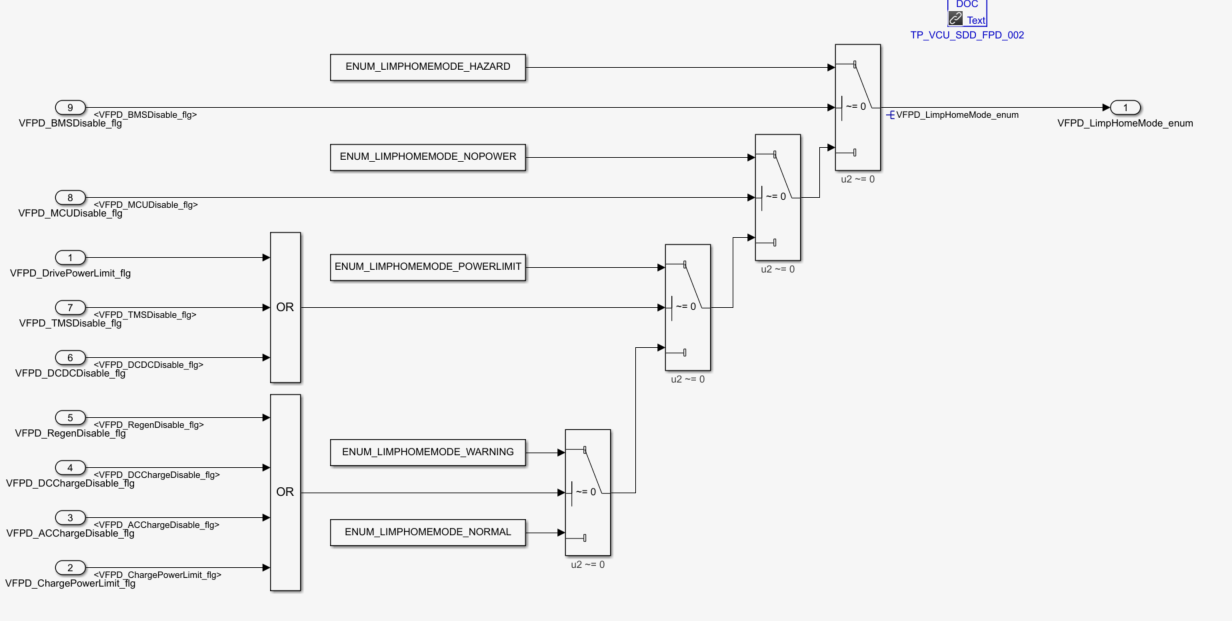
當故障條件成立後，若故障解除需維持故障保護狀態，待關機休眠後重新啟動才可解除。

Table 4‑1故障管理資訊與整車功能關係表

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ＡＣ充電 | ＤＣ充電 | 再生煞車 | 低壓電池充電 | 冷氣及電池包強冷 | 暖氣及電池包加熱 | 動力及電池系統冷卻 | 換檔 | 電機驅動 | 高壓電源輸出 |  |
| 正常 | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | 正常模式 |
| 關閉AC充電 | **N** | Y | Y | Y | Y | Y | Y | Y | Y | Y | 警示模式 |
| 關閉DC充電 | Y | **N** | Y | Y | Y | Y | Y | Y | Y | Y | 警示模式 |
| 關閉Regen | Y | Y | **N** | Y | Y | Y | Y | Y | Y | Y | 警示模式 |
| 充電功率限制 | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | 警示模式 |
| 驅動動力限制 | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | 動力限制模式 |
| 關閉DCDC | Y | Y | Y | **N** | Y | Y | Y | Y | Y | Y | 動力限制模式 |
| 關閉TMS | **N** | **N** | Y | Y | **N** | **N** | **N** | Y | Y | Y | 動力限制模式 |
| 關閉MCU | Y | Y | **N** | Y | Y | Y | Y | **N** | **N** | Y | 無動力模式 |
| 關閉BMS | **N** | **N** | **N** | **N** | **N** | **N** | **N** | **N** | **N** | **N** | 危害模式 |



### ADCU\_SRDS\_02\_001 系統跛行模式判斷



依據上述的功能關閉狀態判斷頗行模式，其優先順序判斷如下：

當VFPD\_BMSDisable\_flg == C\_TRUE，則VFPD\_LimpHomeMode\_enum = ENUM\_LIMPHOMEMODE\_HAZARD。

或VFPD\_MCUDisable\_flg == C\_TRUE ，則VFPD\_LimpHomeMode\_enum = ENUM\_LIMPHOMEMODE\_NOPOWER。

或VFPD\_DrivePowerLimit\_flg == C\_TRUE || VFPD\_DCDCDisable\_flg == C\_TRUE || VFPD\_TMSDisable\_flg == C\_TRUE，則VFPD\_LimpHomeMode\_enum = ENUM\_LIMPHOMEMODE\_POWERLIMIT。

或VFPD\_ACChargeDisable\_flg == C\_TRUE || VFPD\_DCChargeDisable\_flg == C\_TRUE || VFPD\_RegenDisable\_flg == C\_TRUE || VFPD\_ChargePowerLimit\_flg == C\_TRUE，則VFPD\_LimpHomeMode\_enum = ENUM\_LIMPHOMEMODE\_WARNING。

否則VFPD\_LimpHomeMode\_enum = ENUM\_LIMPHOMEMODE\_NORMAL。

Appendix A

無。