BSG 控制器失效注入測試與驗證技術

Fanlt Injection Test and Validation Technology for BSG Controller

陳益新

工研院機械所 智慧車輛技術組 電能系統部

前言

本研究主要針對皮帶式啟動發電機控制器 (belt starter generator controller, 以下簡稱 BSG 控制器) 進行失效注入 (fault injection, FI) 測試、驗證所設計之保護機制，使得產品之功能安全符合所需之汽車安全完整性等級 (automotive safety integrity level, ASIL)；同時於已建立之訊號級動力系統硬體在環驗證平台 (Signal-HIL Verification Platform) 上發展自動化測試程序以縮短測試時程達到節省成本之目的。

一、安全目標展開

本研究主要目的為驗證控制器的硬體安全功能需求，於開發階段遵循 ISO26262 國際標準設計流程；由危害分析與風險評估制定系統安全目標 (safety goal)；接著依序展開驗證動力系統之功能安全需求 (functional safety requirement, FSR)、驗證軟、硬體整合層級之技術實現手段 (technical safety requirement, TSR) 最後再到軟體安全需求 (software safety requirement, SSR) 與硬體安全需求 (hardware safety requirement, HSR) 各自的測試目標。本研究藉由訊號級硬體在環測試方法，透過各種故障的注入以驗證控制器硬體之保護功能。

二、控制器硬體測試與驗證架構

為了精確模擬控制器於真實世界運行時間下發生之失效行為，本研究選用即時模擬器 (real-time simulator) Opal-RT OP5600 作為硬體測試與驗證發展平台；並且於 model-based 的模擬軟體 Matlab/Simulimk 下建立驅動器 (inverter)、動力馬達等受控模型 (plant model) 與失效注入開關 (fault injection matrix)；再將真實控制器與機箱連接形成一條完整的測試迴路，最後利用自行建立之自動化測試程序驗證各項系統保護功能。訊號級控制器硬體在環驗証平台如**圖 1** 所示。

本研究引入 ISO26262 設計開發精神，賦予每項測試案例 (test case) 一個 ID；內容、目標等描述

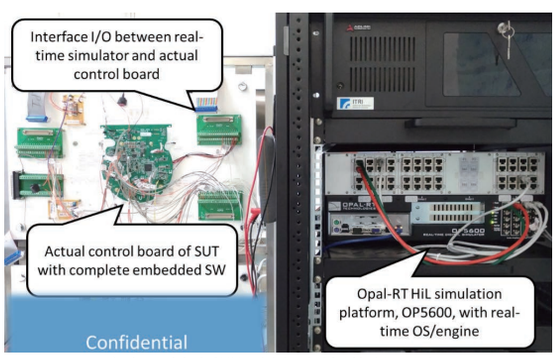

圖 1 控制器系統功能驗證平台

如下所示：

VHSR_01-01：

(a) 驗證 UU 相電流比較器迴路參考訊號等於實際項電流值。

(b) 驗證 UU 相電流過電流保護機制之診斷與反應正確作動。

VHSR_01-02：

(c) 驗證 UD 相電流比較器迴路參考訊號等於實際項電流值。

(d) 驗證 UD 相電流過電流保護機制之診斷與反應正確作動。

VHSR_02-01：

(e) 驗證 VU 相電流比較器迴路參考訊號等於實際項電流值。

(f) 驗證 VU 相電流過電流保護機制之診斷與反應正確作動。

VHSR_02-02：

(g) 驗證 VD 相電流比較器迴路參考訊號等於實際項電流值。

(h) 驗證 VD 相電流過電流保護機制之診斷與反應正確作動。

VHSR_03-01：

(i) 驗證 WU 相電流比較器迴路參考訊號等於實際項電流值。

(j) 驗證 WU 相電流過電流保護機制之診斷與反應正確作動。

VHSR_03-02：

(k) 驗證 WD 相電流比較器迴路參考訊號等於實際項電流值。

(l) 驗證 WD 相電流過電流保護機制之診斷與反應正確作動。

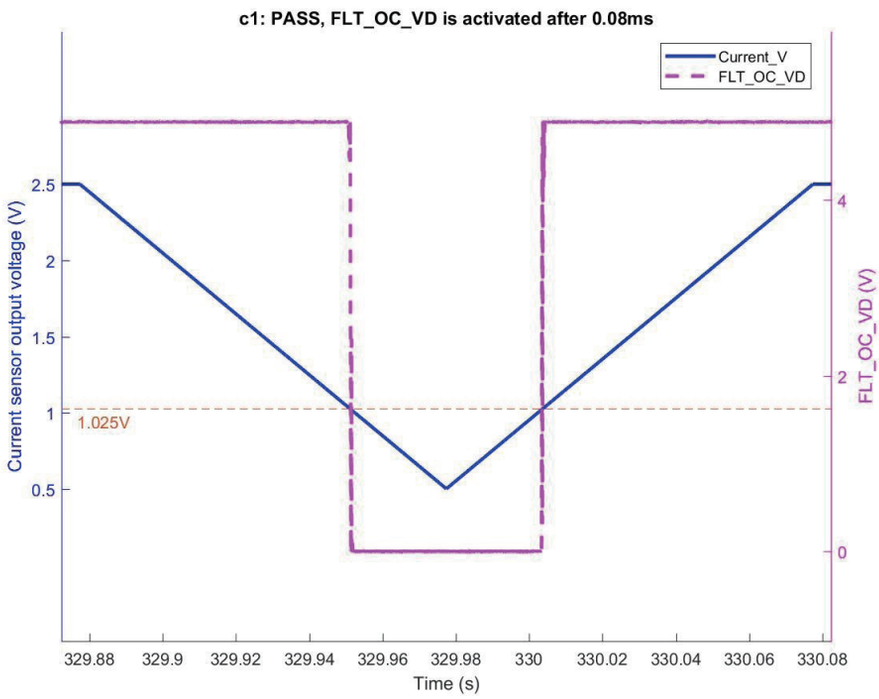

圖 2 判斷準則 C1

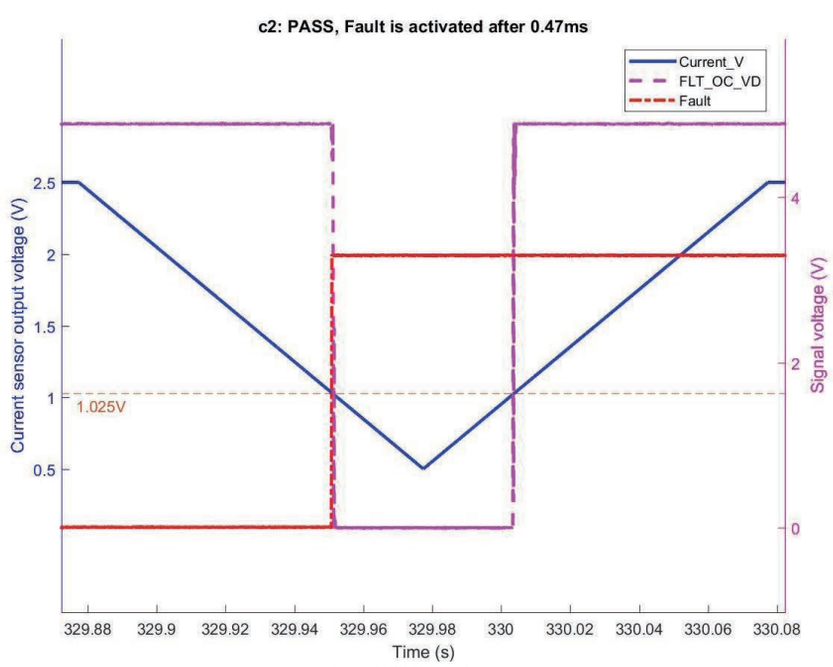

圖 3 判斷準則 C2

更完整的內容

詳見【機械工業雜誌】420 期・107 年 3 月號

機械工業雜誌・每期 220 元・一年 12 期 2200 元

劃撥帳號：07188562 工業技術研究院機械所

訂書專線：03-591-9339

傳真訂購：03-582-2011

機械工業雜誌・官方網站：www.automan.tw

機械工業雜誌・信箱：jmi@itri.org.tw