# 1 | TFC-SPL: DOMAIN ENGINEEERING PHASE

## 1.1 | Tiriba SPL Hazard Analysis and Risk Assessment

During Domain HARA, variation in *No pilot commands* and *Value pilot commands* hazards and their risks were identified in both two aforementioned system variants (see Table 1).

**TABLE 1** Variability on Tiriba flight control SPL HARA and allocation of safety requirements.

| | **Hazard Analysis** | | **Risk Assessment and Allocation of Safety Req.** | | |
|---|---|---|---|---|---|
| **System Variant** | **Hazard Defn.** | **Hazard Causes** | **Severity** | **likelihood** | **DAL** |
| TFC-MAT/<br>Controlled | No pilot commands | Omission-FSC.filteredControls AND<br>Omission-PWMDecoder.flightControls | Catastrophic | $10e - 9$ | A |
| **TFC-ALL/<br>Uncontrolled** | No pilot commands | Omission-FSC.filteredControls AND<br>Omission-PWMDecoder.flightControls AND<br>**Omission-ModeSwitcher.controlMode** | **Hazardous** | **10e-7** | **B** |
| TFC-MAT/<br>Controlled | Incorrect pilot commands | Value-FSC.filteredControls AND<br>Value-PWMDecoder.flightControls | Hazardous | $10e - 7$ | B |
| **TFC-ALL/<br>Uncontrolled** | Incorrect pilot commands | Value-FSC.filteredControls AND<br>Value-PWMDecoder.flightControls AND<br>**Value-ModeSwitcher.controlMode** | **Hazardous** | **10e-5** | **C** |

## 1.2 | Allocation and Decomposition of Safety Requirements

Variation in the DALs allocated to mitigate hazards in both Tiriba system variants has direct impact on the development processes to be enacted to comply with safety standards in order to achieve the safety certification of an individual system variant, as illustrated in Table 2.

**TABLE 2** Variability in safety-critical system development processes per level of integrity.

| | **Standard Requirements** | **Development Assurance Levels** | | | | |
|---|---|---|---|---|---|---|
| **Safety Objectives** | **Activities** | A | **B** | **C** | **D** | **E** |
| The aircraft/system functional hazard is performed with **independence** | SAE ARP 4754A sec. 5.1.1, 5.2.3, 5.2.4 | **v** | **v** | **-** | **-** | **-** |
| The aircraft/system functional hazard is performed | SAE ARP 4754A sec. 5.1.1, 5.2.3, 5.2.4 | **v** | **v** | **v** | **v** | **-** |
| Verification of additional code that cannot be traced to the source code is achieved | DO-178C sec. 6.4.4d: Analysis to confirm that all the test cases are traceable to requirements | **v** | **v** | **-** | **-** | - |
| High level requirements should comply with system requirements | DO-178C sec. 6.3.1: Analysis of compliance with system requirements | **v** | **v** | **v** | **-** | - |

**v** : safety objective and activities are **highly recommended** or **recommended** to achieve the given DAL.

**-** : safety objective and activities are **not required** to achieve the given DAL.

The DALs allocated to TFC hazards can be further decomposed throughout components and their associated failure modes. Table 3 illustrates the decomposition of DALs allocated to *No pilot commands* and *Value pilot commands* in the TFC-MAT system variant (see Table 1) throughout *PWM Decoder* component and its failure modes.

**TABLE 3** Variability in the DAL decomposition throughout components and their failure modes.

| Component | Failure Mode | FM-DAL: TFC-MAT | DAL: TFC-MAT | FM-DAL: TFC-ALL | DAL:TFC-ALL | DAL: SPL |
|---|---|---|---|---|---|---|
| Barometric Processor | OFailure1 | C | C | C | **C** | **C** |
| | OFailure2 | C | | C | | |
| PWM Decoder | **OFailure1** | A | A | **C** | **C** | **A** |
| | **OFailure2** | - | | **C** | | |
| | **VFailure1** | E | | **C** | | |
| | **VFailure2** | - | | **C** | | |

**-** : failure mode is absent in the component in a particular system variant.

### 1.3 | Tiriba SPL Component Fault Modeling

In the TFC-SPL, different component failures may contribute to the occurrence of each identified system hazard in different TFC variants and usage contexts. The component fault modeling was carried out, and 106 failure expressions were added to 47 Tiriba flight control model elements. Table 4 illustrates an example of variation in the specification of component fault models for the BCP component.

**TABLE 4** Variability in component fault analysis and modeling.

| | | Component Failure Data | |
|---|---|---|---|
| **System Variant** | **Component** | **Output Deviation** | **Failure Expression** |
| TFC-MAT/ Controlled | BCP | Omission-*AutopilotSettings* | OFailure1 OR<br>(Omission-*BasicCommand* **OR**<br>Omission-*SensorData*) |
| TFC-ALL/ Uncontrolled | BCP | Omission-*AutopilotSettings* | OFailure1 OR<br>(Omission-*BasicCommand* **AND**<br>Omission-*SensorData*) |
| | | Omission-*Mode* | OFailure2 OR<br>(Omission-*BasicCommand* AND<br>Omission-*SensorData*) |

## 2 | TFC-SPL: APPLICATION ENGINEERING PHASE

### 2.1 | Tiriba Product Hazard Analysis

Table 5 shows an excerpt of TFC-MAT variant-specific hazard analysis Thus, a delay in receiving pilot commands, with *catastrophic* severity and *low* likelihood (10e-9 per hour of operation), can emerge due the occurrence of *late* failures in both *FSC* and *PWM Decoder* component *outputs* in the TFC-MAT system variant when operating under *stormy* weather conditions. On the other hand, the occurrence of an *early* failure in the *FSC.filteredControls* output or a *commission* failure in the *PWMDecoder.flightControls* output can lead to the *reception of pilot commands earlier as intended* system hazard, with a *hazardous* severity and a probability of occurrence of 10e-7 per hour of operation, when TFC-MAT is assumed to operate under *rainy* weather conditions.

**TABLE 5** Application-specific HARA and allocation of safety requirements.

| | **Hazard Analysis** | | **Risk Assessment and Allocation of Safety Req.** | | |
|---|---|---|---|---|---|
| **Variant/Context** | **Hazard Defn.** | **Hazard Causes** | **Severity** | **likelihood** | **DAL** |
| TFC-MAT/ Stormy | Delay in receiving pilot commands | Late-FSC.filteredControls AND Late-PWMDecoder.flightControls | Catastrophic | $10e-9$ | A |
| TFC-MAT/ Rainy | Pilot commands received earlier as intended | Early-FSC.filteredControls OR Commission-PWMDecoder.flightControls | Hazardous | $10e-7$ | B |

## 2.2 | Tiriba Product Component Fault Modeling

Table 6 shows the enhanced Tiriba BCP component fault model with additional *output deviations* that may contribute to the occurrence of two additional TFC-MAT application-specific hazards identified during application HARA (see Table 5).

**TABLE 6** Application-specific component fault modeling.

| | | **Component Failure Data** | |
|---|---|---|---|
| **Variant/Context** | **Component** | **Output Deviation** | **Failure Expression** |
| TFC-MAT Stormy | BCP | Late-*AutopilotSettings* | OFailure1 OR (Late-*BasicCommand* OR Late-*SensorData*) |
| | | Commission-*AutopilotSettings* | CFailure1 OR (Early-*BasicCommand* OR Commission-*SensorData*) |

## 2.3 | Tiriba Fault Trees and FMEA Synthesis

Table 7 shows the FMEA results for the Tiriba *PWM Decoder* subsystem component, which might change according to the targeted product variant.

**TABLE 7** Variability in Failure Modes and Effects Analysis.

| System Variant | Component | Failure Mode | System Effect | Single Point of Failure |
|---|---|---|---|---|
| TFC-ALL Controlled | PWM Decoder | *OFailure1* | *No pilot commands* | False |
| | | ***OFailure2*** | ***No pilot commands***<br>***Value pilot commands*** | ***False*** |
| | | *VFailure1* | *Value pilot commands* | ***False*** |
| | | ***VFailure2*** | ***Value pilot commands*** | ***False*** |
| TFC-MAT Controlled | PWM Decoder | *OFailure1* | *No pilot commands* | False |
| | | *VFailure1* | *Value pilot commands* | ***True*** |