RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

8/10/2016

SAFETY SYSTEM DIGITAL PLATFORM
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -
TOPICAL REPORT

Mitsubishi Electric Corporation

TAC NO.:	**MF4228**
RAI NO.:	**#1**
DATE OF RAI ISSUE:	**6/29/2016**

QUESTION NO.: 9 for JEXU-1041-1008, “Safety System Digital Platform – MELTAC”

Page 214 of the TR discusses the generic redundant parallel controller reliability analysis and a fault tree analysis to support that controller configuration review. The NRC staff needs to review this specific analysis and additional analyses for other controller configurations and modules that are included in the MELCO platform to complete its evaluation in accordance with ISG-06 Section D.9.4.2.1.1. Please provide a description of the criteria used to determine which controller configuration will be used (i.e. single, redundant parallel or redundant standby) as well as documentation to demonstrate compliance of other possible controller configurations to this criteria.

ANSWER:

ISG-06 Section D.9.4.2.1.1, “Failure Modes and Effects Analysis (FMEA)” does not pertain to reliability, which is the subject of page 214 of the Topical Report (i.e., Controller Reliability Analysis). The FMEA is conducted to demonstrate that there are no single failures that can adversely affect the safety function in multiple safety divisions, and that there are no undetectable failures that could accumulate to result in failure of multiple safety divisions. The FMEA does not consider the frequency of failures. The FMEA method for MELTAC is described in Section 7.3 of the Topical Report.

Section 7.2, “Controller Reliability Analysis” pertains to frequency of failures for the three controller configurations that can be applied with MELTAC. These are single, redundant parallel, and redundant standby (described in Section 4.1.1).
Among these configurations, the configuration that can satisfy the plant specific reliability requirements is applied, with consideration of both actuation assurance and spurious actuation prevention. The actual reliability calculations are in plant specific documentation. The reliability models shown in Section 7.2 are intended to only show the reliability analysis method for each of the three basic controller configurations.
The reliability models of these configurations are shown in Figure 1, Figure 2 and Figure 3, respectively.

Each configuration has one input module and one output module as a single I/O module. Redundant I/O modules can also be applied, as described in Section 4.1.1; for simplicity, these reliability models show only single I/O modules.

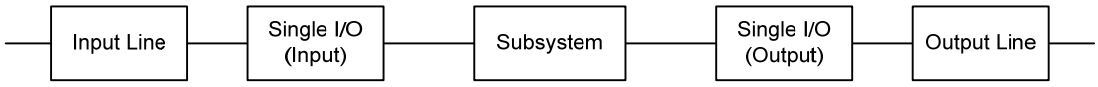


Figure 1 Reliability Model of a Single Controller

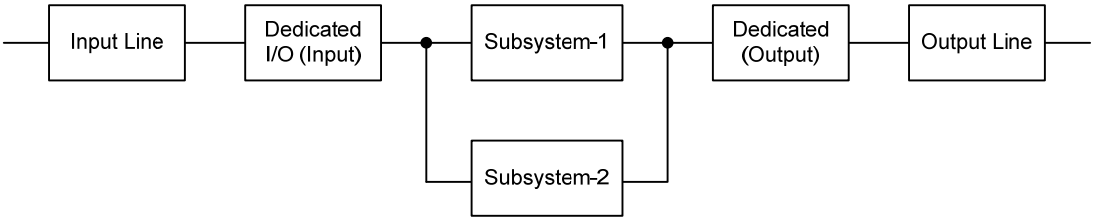


Figure 2 Reliability Model of a Redundant Parallel Controller

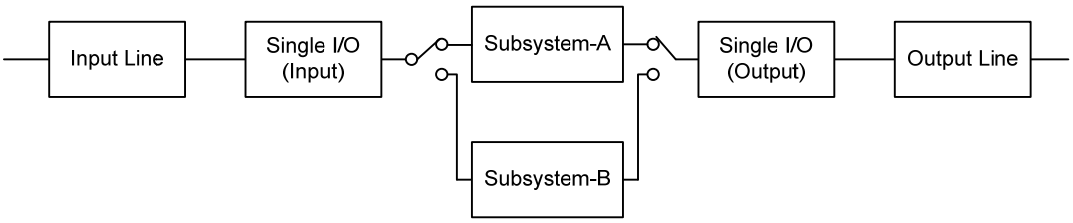


Figure 3 Reliability Model of a Redundant Standby

A comparison of the three controller subsystem configurations is described below. This comparison excludes the reliability of the single I/O modules, which is common to each configuration.

a) Spurious actuation

The continuous self-testing will shut down the single controller for most faults that could result in spurious actuation. Prevention of spurious actuation is not improved through the redundant standby controller configuration, which is equivalent to the single controller configuration. The likelihood of spurious actuation of the redundant parallel configuration is increased by 100% compared to the single and standby redundant configurations if the outputs are in a 1-out-of-2 configuration. However, if those outputs are in a 2-out-of-2 configuration to prevent spurious actuation, then the probability of spurious actuation is 50% of the single controller. And the outputs in a 2-out-of-2 configuration will be better than the single controller configuration because it can prevent spurious actuation caused by all failures in one of the two controllers.

$$F_{(\text{Redundant Parallel (2-out-of-2)})} < F_{(\text{Single})} = F_{(\text{Redundant Standby})} < F_{(\text{Redundant Parallel (1-out-of-2)})}$$

b) Failure to actuate

The redundant standby controller has almost the same reliability as the single controller. The reliability is limited primarily by the coverage of continuous self-testing, which is close to, but not 100%.The probability of failure to actuate of the redundant parallel controller is twice of the single controller when these outputs are 1-out-of-2. However, if those outputs are in a 2-out-of-2 configuration to prevent spurious actuation, then the probability of failure to actuate is 50% of the single controller.

$$U_{(\text{Redundant parallel (1-out-of-2)})} < U_{(\text{Redundant standby})} < U_{(\text{Single})} < U_{(\text{Redundant parallel (2-out-of-2)})}$$

Other configurations of MELTAC controllers are possible for plant specific applications. However, those configurations would be comprised of one or more of the three configurations described above, with the inputs shared and the outputs combined on the field side of the I/O modules using hardwired connections.

The FTAs for each controller configuration will be added to the Topical Report.

Impact on Topical Report
The answer above will be added to Section 7.2 of the Topical Report. See Attachment-1.

7.2 Controller Reliability Analysis

The failure rate of any safety-related system where MELTAC platform is applied as a whole, depends on the configuration of the entire system. Variations for each application include:

- The number and configuration of redundant divisions
- The number and configuration of controllers within each division
- The redundancy within each controller
- The configuration of I/O modules and Communication Interface Modules and the significance of these interfaces to the safety function (i.e.: the safety function logic design)

~~This section describes a method used to determine the reliability of a generic redundant parallel controller. The method for single controller architecture can be extrapolated from this method.~~ ToR-9

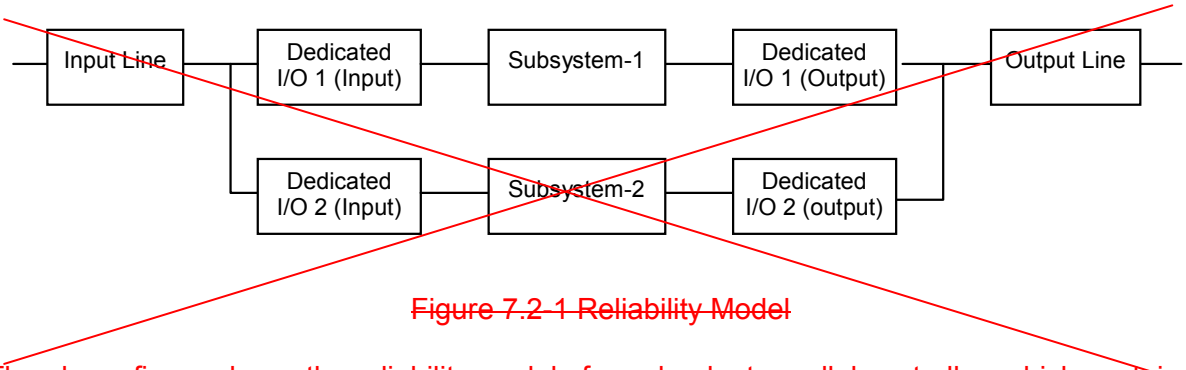
The controller reliability analysis is performed as follows.

- A reliability model for the system's safety function is generated
- The fault tree analysis (FTA) of this reliability model is performed to determine the frequency of:
  - Spurious actuation of the safety function
  - Failure to actuate the safety function

~~The reliability model of a simple system is shown in Section 7.2.1. As an example of the reliability analysis process, Figure 7.2-2 shows the fault tree for spurious actuation of the safety function. The FTA for spurious actuation is explained below.~~ ToR-9

The three controller configurations that can be applied with MELTAC are described in section 4.1.1. These are single controller, redundant parallel and redundant standby controller. Among those three, the configuration that can satisfy the plant specific reliability requirements is applied, with consideration of both actuation assurance and spurious actuation prevention.

7.2.1 Reliability Model



~~Figure 7.2-1 Reliability Model~~

~~The above figure shows the reliability model of a redundant parallel controller, which contains one input module and one output module in each subsystem.~~
~~In the reliability model, the Status Display Module is not contained in the subsystem, because the Status Display Module only displays the current state of the subsystem and its failure does not affect the safety function of the subsystem. The Control Network I/F Module and the Optical Switch Module are not contained in this simplified system. They would be included, depending on how the data from the Control Network is used in the application software. This also applies to the Data Link interface from the Bus Master Modules.~~ ToR-9
The reliability models of the single controller, redundant parallel and redundant standby controller are shown in Figure 7.2-1, Figure 7.2-2 and Figure 7.2-3 respectively.

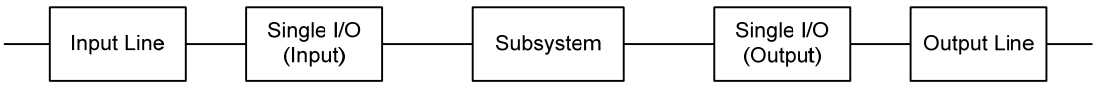


Figure 7.2-1 Reliability Model of a Single controller 3

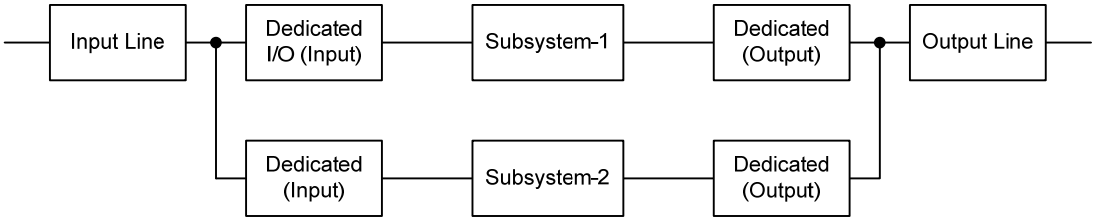


Figure 7.2-2 Reliability Model of a Redundant Parallel

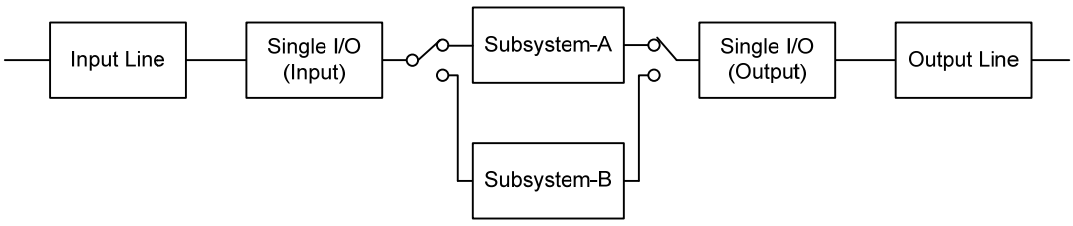


Figure 7.2-3 Reliability Model of a Redundant Standby

A comparison of the three controller subsystem configurations is described below.

a) Spurious actuation

ToR-9

The continuous self-testing will shut down the single controller for most faults that could result in spurious actuation. Prevention of spurious actuation is not improved through the redundant standby controller configuration, which is equivalent to the single controller configuration. The likelihood of spurious actuation of the redundant parallel configuration is increased by 100% compared to the single and standby redundant configurations if the outputs are in a 1-out-of-2 configuration. However, if those outputs are in a 2-out-of-2 configuration to prevent spurious actuation, then the probability of spurious actuation is 50% of the single controller. And the outputs in a 2-out-of-2 configuration will be better than the single controller configuration because it can prevent spurious actuation caused by all failures in one of the two controllers.

$$F_{(\text{Redundant Parallel (2-out-of-2)})} < F_{(\text{Single})} = F_{(\text{Redundant Standby})} < F_{(\text{Redundant Parallel (1-out-of-2)})}$$

The FTAs for each controller configuration are shown in the Figure 7.2-4 to Figure 7.2-6.

b) Failure to actuate

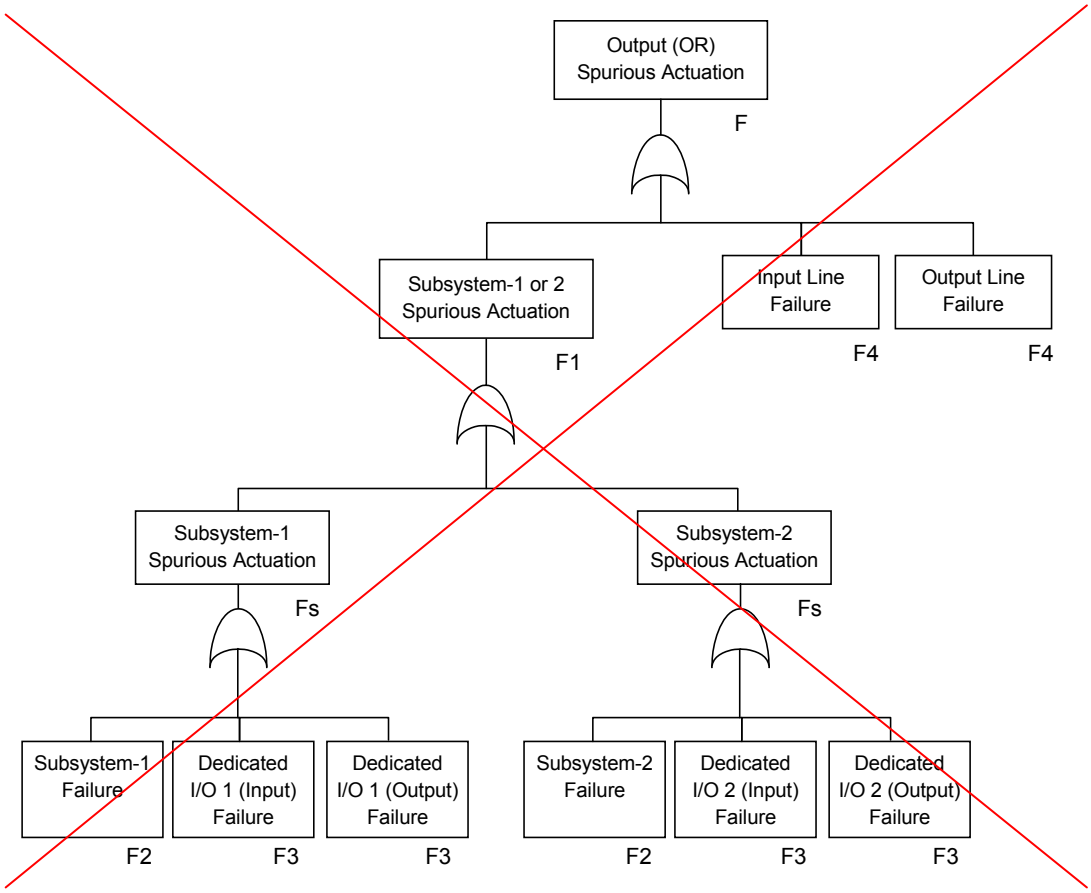
The redundant standby controller has almost the same reliability as the single controller. The reliability is limited primarily by the coverage of continuous self-testing, which is close to, but not 100%.The probability of failure to actuate of the redundant parallel controller is twice of the single controller when these outputs are 1-out-of-2. However, if those outputs are in a 2-out-of-2 configuration to prevent spurious actuation, then the probability of failure to actuate is 50% of the single controller.

$$U_{(\text{Redundant parallel (1-out-of-2)})} < U_{(\text{Redundant standby})} < U_{(\text{Single})} < U_{(\text{Redundant parallel (2-out-of-2)})}$$

The FTAs for each controller configuration are shown in the Figure 7.2-7 to Figure 7.2-9.

Other configurations of MELTAC controllers are possible for plant specific applications. However, those configurations would be comprised of one or more of the three configurations described above, with the inputs shared and the outputs combined on the field side of the I/O modules using hardwired connections.

7.2.2 ~~FTA of~~ Spurious Actuation ~~of the Safety Function~~



~~Figure 7.2-2 Fault Tree for Output Failure Spurious Actuation~~

~~Regarding the cause of spurious actuation, the failure rate is described below.~~

~~F = F1 + F4 + F4~~
~~F1 = Fs + Fs~~
~~Fs = F2 + F3 + F3~~

~~Failure rate Fi (i = 1,2,3…) causes spurious action of each module or subsystem and is defined below.~~

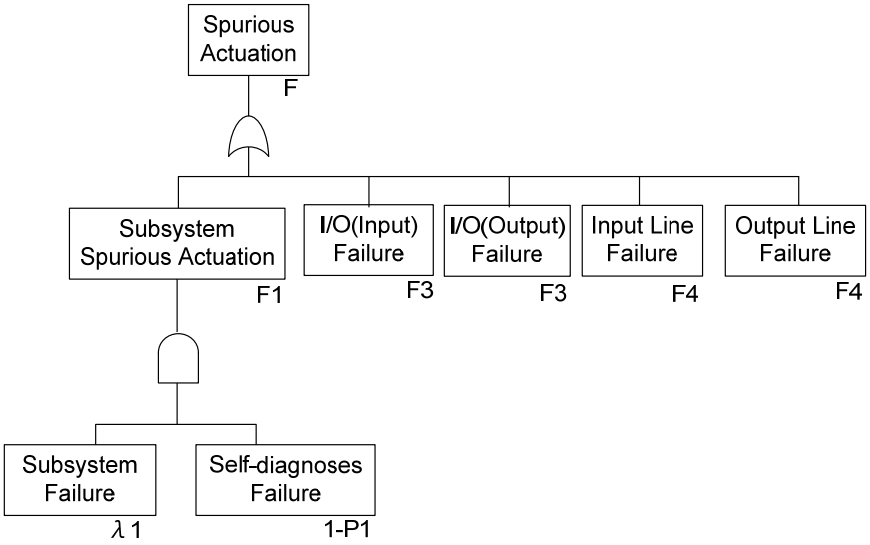
~~Fi = λ i x (1-Pi)~~
~~λ i = failure rate~~
~~Pi = probability of detecting the failure which affects the safety function through self-diagnosis~~

~~Calculations of F2, F3 and F4 are described in Sections 7.2.4.1, 7.2.4.2 and 7.2.4.3.~~
~~The failure rates of the Input Line and the Output Line are the same, because they consist of the same module and unit.~~

ToR-9

~~This FTA model assumes this very simple system, in which an input directly affects a system output. Systems with more complex logic may validate inputs (e.g.: voting) within the application logic so that spurious actuation requires multiple input failures.~~
The Figure 7.2-4, Figure 7.2-5, and Figure 7.2-6 show the FTA for spurious actuation of single controller, redundant standby and redundant parallel respectively.

The redundant standby configuration has Status Display and Switch Module. However it is not considered in this analysis because the failure of the Status Display and Switch Module doesn't cause the loss of safety function and subsystem switch function.



ToR-9

Figure 7.2-4 Fault Tree for Spurious Actuation of Single Controller

Regarding the cause of spurious actuation of the single controller, the failure rate is described below.

$F_{(Single)} = F1 + F3 + F3 + F4 + F4$

Failure rate Fi (i = 1,2,3···) causes spurious action of each module or subsystem and is defined below.

$Fi = \lambda i \times (1-Pi)$

λi = failure rate

Pi = probability of detecting the failure which affects the safety function through self-diagnosis

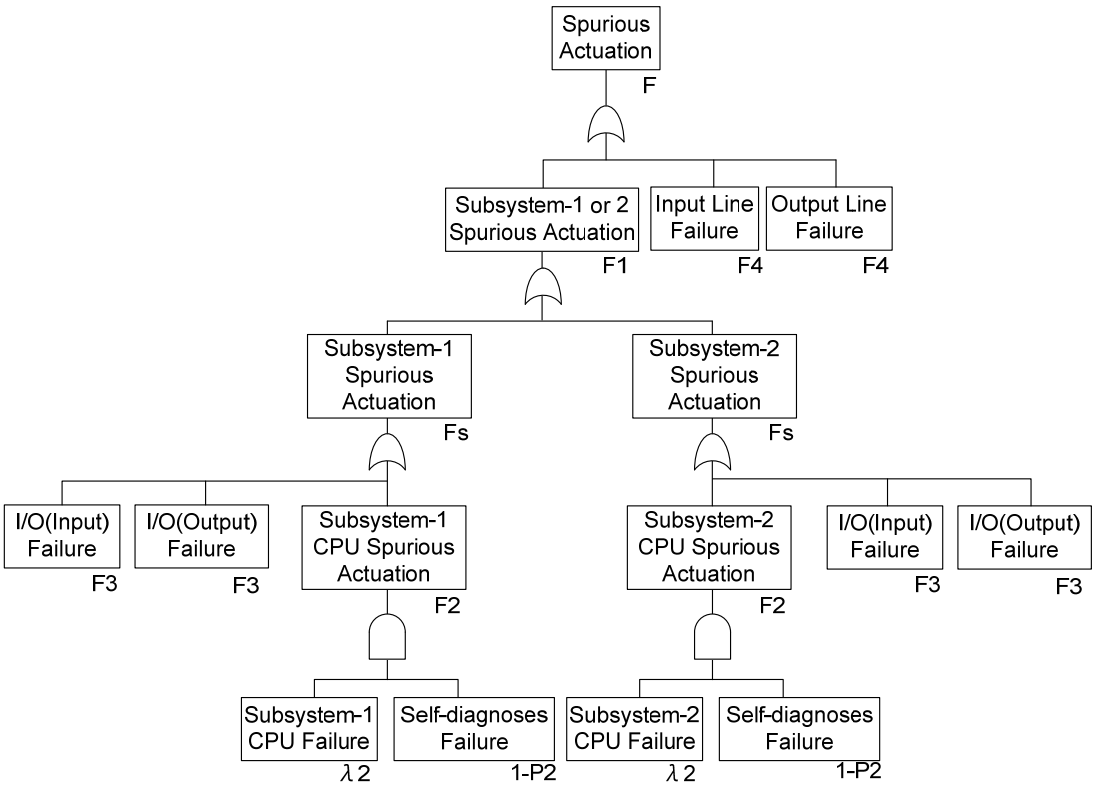


Figure 7.2-5 Fault Tree for Spurious Actuation of Redundant Parallel

ToR-9

Regarding the cause of spurious actuation of the redundant parallel whose output is 1 out of 2, the failure rate is described below.

$F_{(Redundant\ Parallel)} = F1 + F4 + F4$
$F1 = Fs + Fs$
$Fs = F2 + F2 + F3$

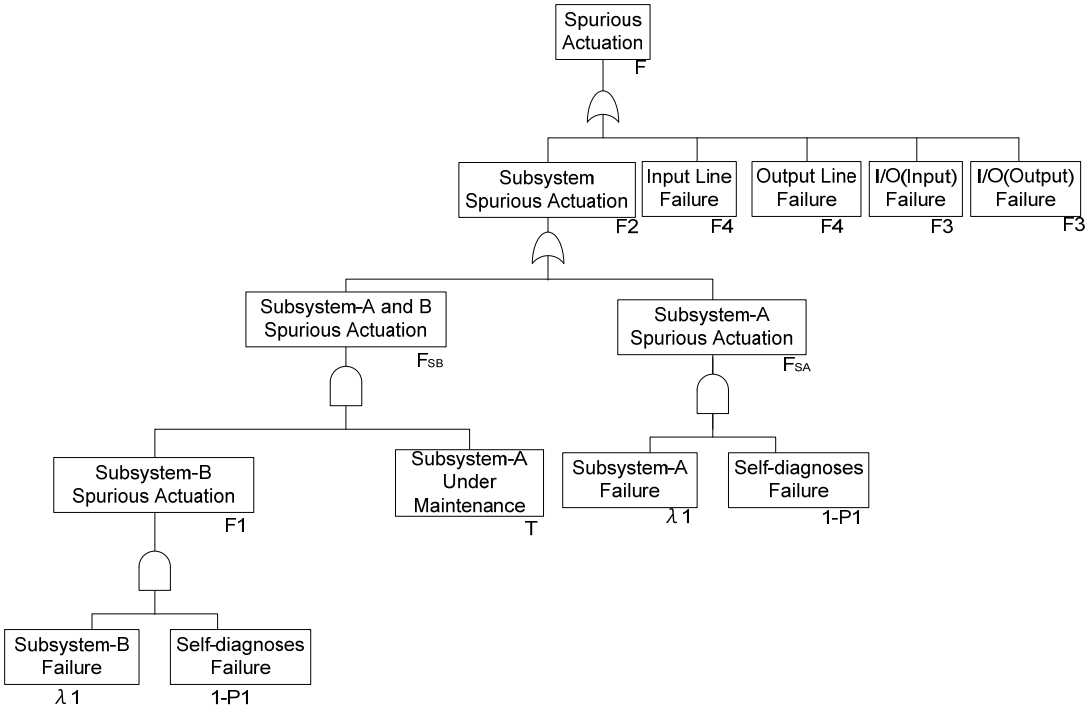


Figure 7.2-6 Fault Tree for Spurious Actuation of Redundant Standby

ToR-9

Regarding the cause of spurious actuation of the redundant standby, the failure rate is described below.

$F_{(Redundant\ Standby)} = F2 + F3 + F3 + F4 + F4$
$F2 = F_{SA} + F_{SB}$
$F_{SA} = F1\ (=\lambda i \times (1-Pi))$
$F_{SB} = F1 \times T$

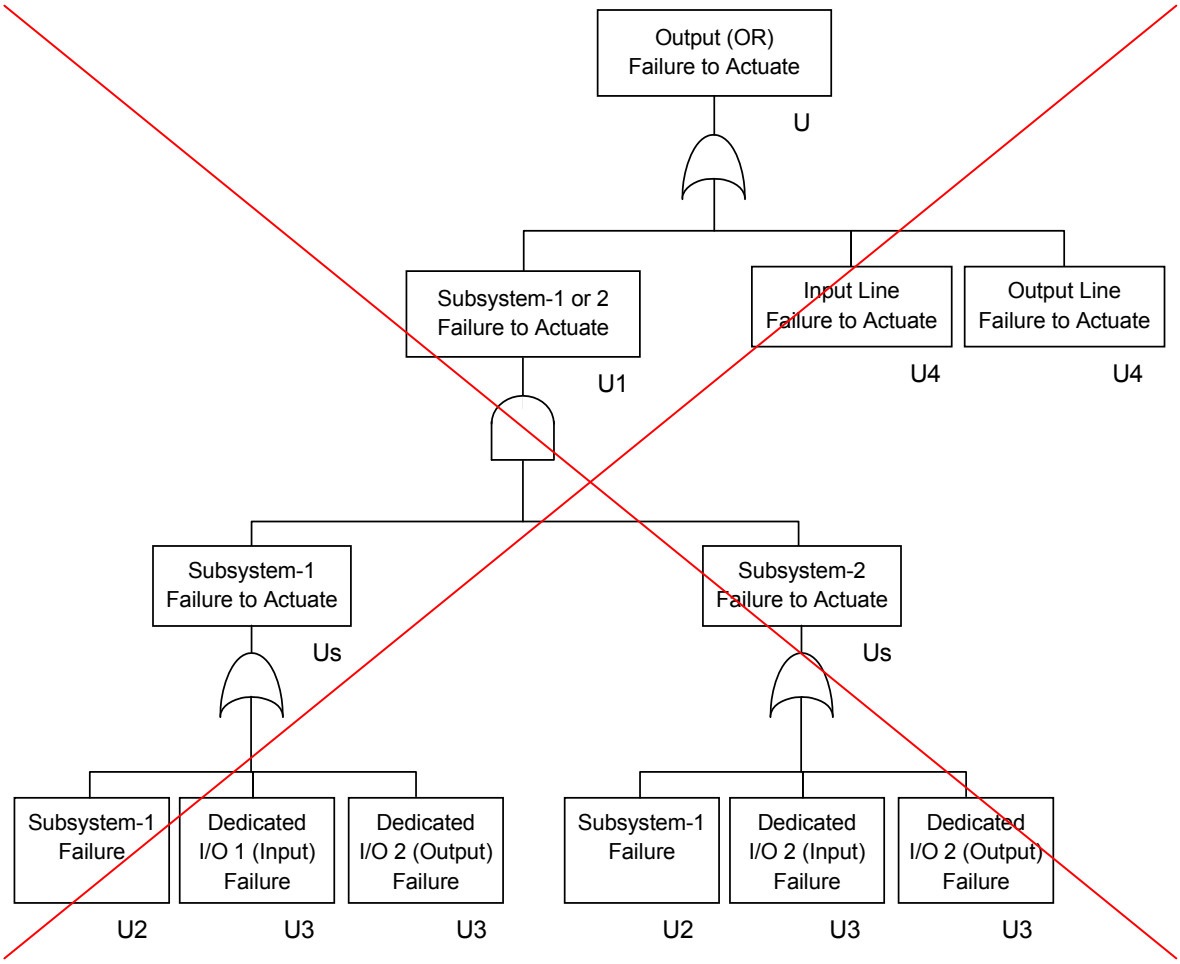
T stands for period of the maintenance of subsystem-A

$T = MTTR / (MTBF + MTTR)$

Since MTTR << MTBF, T can be considered as closely 0.
Therefore, the spurious actuation is provided as follows, because F2 = F1.

$F_{(Redundant\ Standby)} = F1 + F3 + F3 + F4 + F4$

7.2.3 ~~FTA of~~ Failure to Actuate ~~the Safety Function~~



~~**Figure 7.2-3 Fault Tree for Failure to Actuate**~~

~~Regarding the cause of failure to actuate, unavailability is described below.~~

~~U = U1 + U4 + U4~~
~~U1 = Us x Us~~
~~Us = U2 + U3 + U3~~

~~Ui is the unavailability of each module or subsystem and is defined below.~~
~~Ui = 1 - MTBF / (MTBF + (1 - Pi) x (Ti /2) + MTTR)~~
~~Ti = Manual test interval~~
~~MTBF = 1 / λi~~

~~Ti and Mean Time To Repair (MTTR) are unique to each application.~~

ToR-9

The Figure 7.2-7, Figure 7.2-8, and Figure 7.2-9 show the FTA for failure to actuate of single controller, redundant standby and redundant parallel respectively.

The failure rate of the Status Display and Switch Module is not considered to this analysis because of the same reason of analysis for spurious actuation.

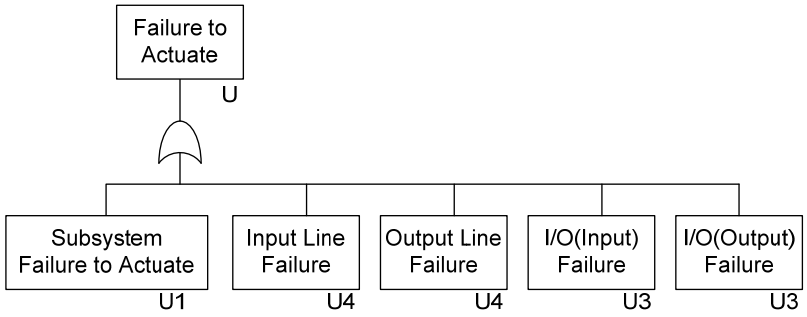


Figure 7.2-7 Fault Tree for Failure to Actuate of Single controller

ToR-9

Regarding the cause of failure to actuate of the single controller, unavailability is described below.

$$U_{(Single)} = U1 + U3 + U3 + U4 + U4$$

Ui is the unavailability of each module or subsystem and is defined below.

Ui = 1 - MTBF / (MTBF + (1 - Pi) x (Ti /2) + MTTR)
Ti = Manual test interval
MTBF = 1 / λi
Ti and Mean Time To Repair (MTTR) are unique to each application.

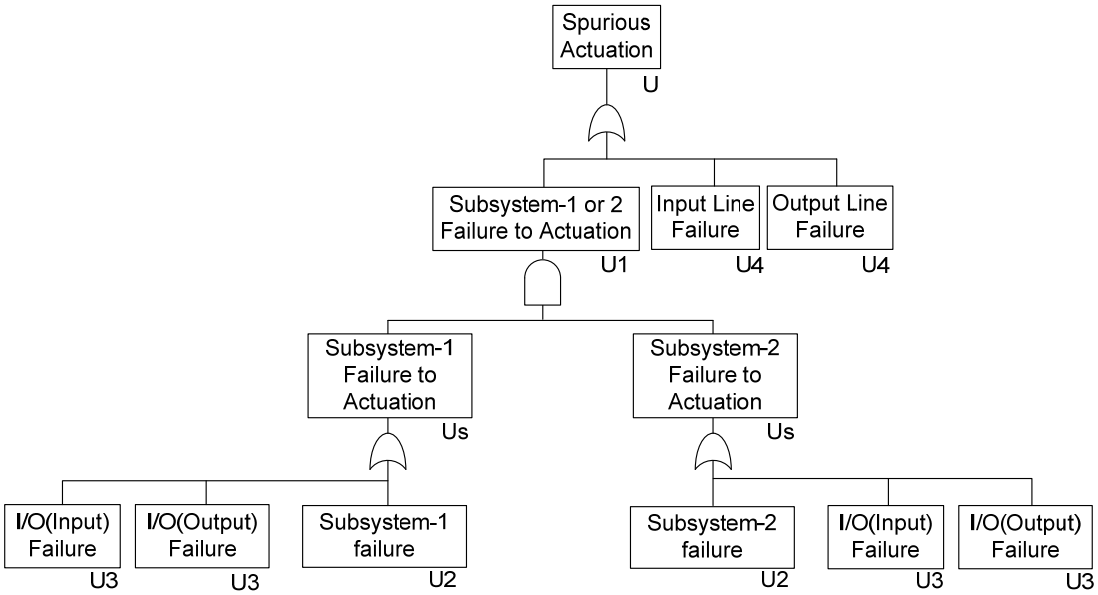
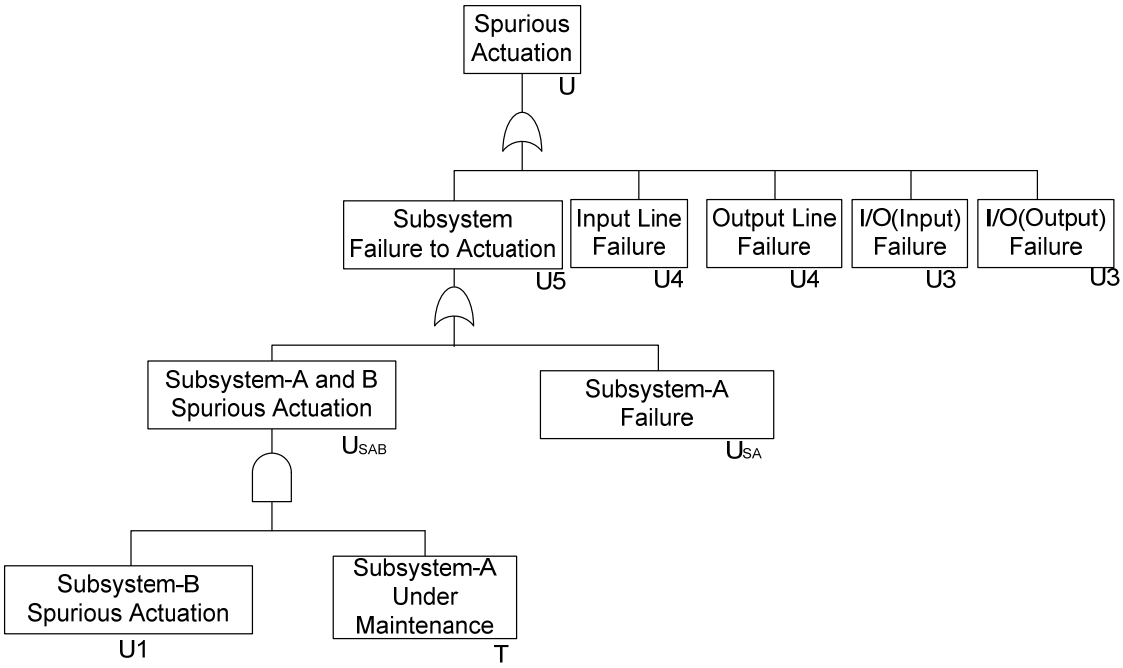


Figure 7.2-8 Fault Tree for Failure to Actuate of Redundant Parallel

ToR-9

Regarding the cause of failure to actuate of the redundant parallel controller, unavailability is described below.

U(redundant parallel) = U1 + U4 + U4
U2 = Us + Us
Us = U2 + U3 + U3



7.2-9 Fault Tree for Failure to Actuate of Redundant Standby

Regarding the cause of failure to actuate of the redundant standby controller, unavailability is described below.

U(redundant standby) = U5+ U3 + U3 + U4 + U4
U5 = U_{SA} +U_{SAB}
U_{SA} = 1- MTBF / (MTBF + (1-P5)x (T5 / 2)) (note)
UA_{SB} = U1 x T

T stands for period of the maintenance of subsystem-A
T = MTTR / (MTBF + MTTR)

Since MTTR << MTBF, T can be considered as closely 0.
Therefore, the spurious actuation is provided as follows, because U5=USA.

U(redundant standby) = USA + U3 + U3 + U4 + U4 (note)

(Note)
USA is the unavailability of the subsystem when the other subsystem is not in failure mode.
USA is provided as above because when the other subsystem is not in failure mode, MTTR can be considered as 0.