Figure 4.1-16 Remaining Time Diagnosis

[

DCD_07.01-46 S01

]

4.1.5 Self-Diagnosis

The MELTAC platform controller is equipped with three types of self-diagnosis features: a hardware based detection process, a software based detection process, and a combination thereof. When an error is detected, an alarm is generated. When the error is severe, the controller makes a transition from the Control or Standby mode to the Failure mode.

Detailed error descriptions are provided in Sections 4.1.5.2 thru 4.1.5.6. The categorization of each error is shown in parenthesis, for example “Clock check (Failure)”.
All errors in Sections 4.1.5.2 and 4.1.5.3 are severe and are therefore categorized as “Failure”. These errors stop main CPU operation, and generate signals that can be used for alarms. All other errors (those identified in Sections 4.1.5.4 and 4.1.5.5) generate signals that can be used for alarms, but do not stop the main CPU operation.

The WDT architecture and error detection process (including the behavior after error detection) of the MELTAC platform is described in Section 4.1.5.7. DCD_07.01-46 DCD_07.01-46 S01

All error signals are identified on the MELTAC engineering tool. The specific grouping of error signals into operator alarms is application specific. Since most applications have redundant CPUs, typically all error signals are grouped to a single operator alarm and then the MELTAC engineering tool is used for diagnosis of specific error conditions.

Failure notice is provided to the plant monitoring system for the three types of errors, ”Failure”, “Alarm”, and “I/O Alarm”. These error signals are typically grouped into system trouble alarms, however the method used to present this information to the operator from the plant monitoring system is application dependent and not within the scope of the MELTAC platform.
Detailed information for diagnosis of all error conditions is provided on the MELTAC engineering tool.

a) Hardware based detection process

With this feature, self-diagnosis is implemented by special diagnostic circuitry on the CPU Module. The feature involves a ~~watchdog timer~~WDT, parity error, timeout, analog input check, etc. DCD_07.01-46 S01
The diagnosis of these features is performed by dedicated hardware device (*1) other than CPU device and is independent of the CPU software (basic and application). DCD_07.01-46
*1) The special diagnostic circuitry consists of hard-wired circuits, FPGA device, or combination of both. DCD_07.01-46 S01

b) Software based detection process

With this feature, self-diagnosis is implemented using the CPU software. The feature involves CPU health~~y~~ check, ROM error check, RAM error check, etc. DCD_07.01-46 S01

c) Software/hardware combination

With this feature, circuitry that supports self-diagnosis is added to the controller and self-diagnosis is performed using software-based read/write operations. This feature involves a digital input check, digital/analog output read-back check, etc.

The controller is monitored based on the above self-diagnosis processes every Execution Cycle. The individual error items can be identified by viewing the LED display on the front of each module and the representative alarm display (Failure, Alarm, I/O Alarm) on the Status Display & Switch Module and by using the MELTAC engineering tool connected via the Maintenance Network.

Each detected error is categorized into the three types (Failure, Alarm and I/O Alarm) as below.

1) Failure
The fatal abnormality by which the subsystem cannot continue its functions is categorized as the Failure.
When the subsystem detects this type of error, it transitions to the Failure mode.
[

]
In the Failure mode, on the other hand, the processing of input/output and operation are stopped, although the processing of sending the own status data of the Failure mode is continued.
[

]
In case of redundant standby controller configuration, when the subsystem in the Control mode changes to the Failure Mode and the subsystem in the Standby mode changes from the Standby Mode to the Control Mode and continues the control function.

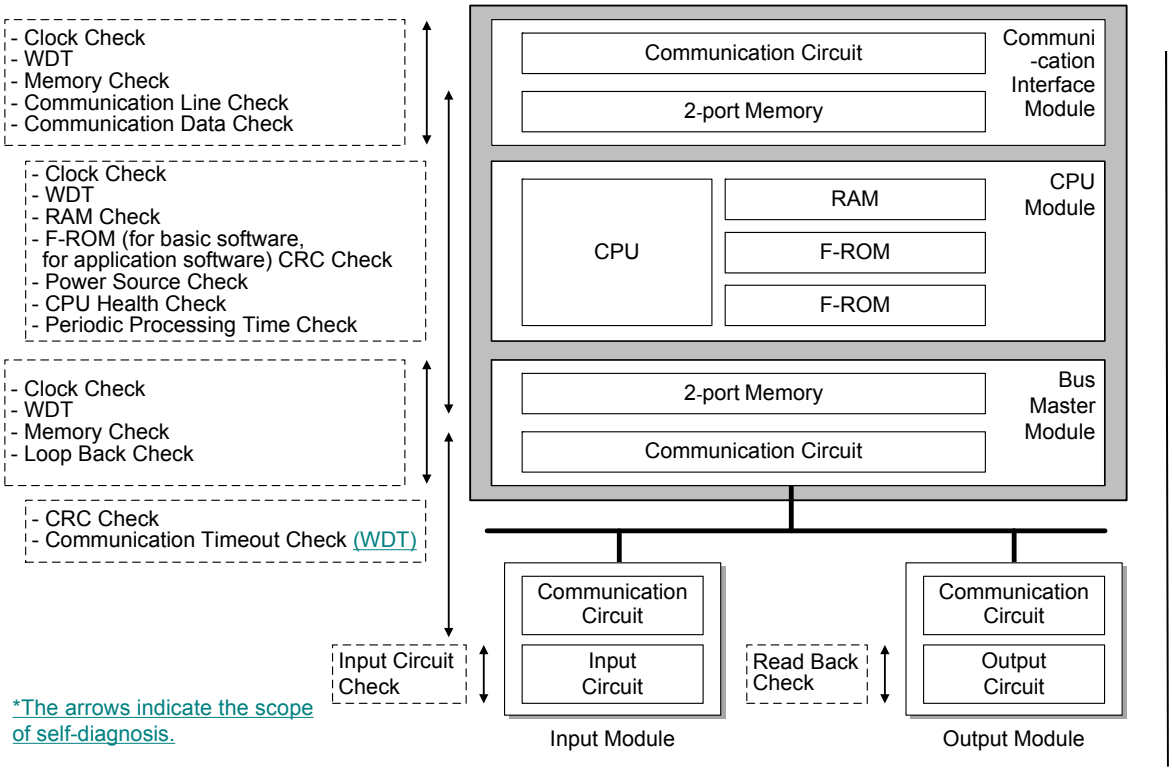
When there is no subsystem which communicates with the controller's Output Module, the Output Module transitions to the Failure mode which is "as-is mode" or "off mode". This mode is specified and a predetermined failure mode output value set on the output module during the loading of the application software to MELTAC platform ~~preset at the application level~~. See 4.1.5.5.2.b for details. DCD_07.01-46 DCD_07.01-46 S01

2) Alarm
The minor abnormality with which the subsystem can continue its functions is categorized as the Alarm. This includes the error of the controller cabinet.
When the subsystem detects this type of error, it does not change its mode and only warns of the alarm. This abnormality is communicated to other systems for alarming via Data Link or the Control Network, as configured at the application level.

3) I/O Alarm
The abnormality of I/O is categorized as the I/O Alarm.
When the subsystem detects this type of error, it does not change its mode and only warns of the alarm. This abnormality is communicated to other systems for alarming via Data Link or the Control Network, as configured at the application level.

4.1.5.1 Coverage of Self-diagnosis

Coverage of self-diagnosis of the controller is shown in Figure 4.1-17.



DCD_07.01-46 S01

Figure 4.1-17 Coverage of Self-Diagnosis Function of the Controller

4.1.5.2 Self-diagnosis of the Controller

The self-diagnosis of the processor modules is described below.
Each diagnosis item is shown with the timing of diagnosis classified as follows:
- Initialization: At the time of initialization
- Self-diagnosis: Once per cycle in the constant cycle operation
- Remaining Time Diagnosis: Periodically in the remaining time of constant cycle operation, but not every cycle.
- Constant: On a constant basis by Hardware

The term “hardware check” used in this section refers to the check process described in Section 4.1.5, “a) Hardware based detection process”.
The term “software check” used in this section refers to the check process described in Section 4.1.5, “b) Software based detection process”.

DCD_07.01-46 S01

4.1.5.2.1 CPU Module

[

DCD_07.09-27 S01
DCD_07.01-46
DCD_07.01-46 S01

DCD_07.01-46
DCD_07.01-46 S01
DCD_07.09-27 S01

]

[

DCD_07.01-46
DCD_07.01-46 S01

DCD_07.
09-27 S01

]

4.1.5.2.2 Bus Master Module

[

DCD_07.
01-46 S01

DCD_07.
01-46

DCD_07.
01-46 S01

DCD_07.
01-46 S01

DCD_07.
09-27 S01

DCD_07.
01-46 S01

DCD_07.
09-27

DCD_07.
09-27

]

4.1.5.2.3 Control Network I/F Module

[

DCD_07.
09-27 S01

DCD_07.
01-46 S01

DCD_07.
01-46 S01

4.1.5.5 Self-diagnosis of I/O Modules

The self-diagnosis of the I/O Modules is described below.

4.1.5.5.1 Input Module

[

DCD_07.
01-46 S01

DCD_07.
01-46 S01

DCD_07.
09-27

]

4.1.5.5.2 Output Module

[

DCD_07.
01-46 S01

DCD_07.
01-46

DCD_07.
01-46 S01

DCD_07.
01-46 S01

DCD_07.
01-46

DCD_07.
01-46 S01

DCD_07.
01-46 S01

4.1.5.7 Watchdog Timer (WDT)

This section provides a description of the WDT architecture and how WDT timeouts~~errors~~ are processed in the MELTAC modules.~~ [~~

~~]~~

DCD_07.01-46
DCD_07.01-46 S01

4.1.5.7.1 Architecture of the WDT

~~The following describes the detailed WDT mechanism. Figure 4.1-18 shows the WDT mechanism, taking the CPU Module as an example. The left side of the figure represents the elements related to the WDT in the CPU Module. The right side of the figure shows the WDT behavior, regarding count up, counter reset, and timeout when the counter value reaches a predefined value.~~
~~The flow of the WDT operations and controls is as follows:~~

DCD_07.01-46

This section provides descriptions of the following:
・Function of the WDT
・Behavior of safety function operation after WDT timeout

DCD_07.01-46
DCD_07.01-46 S01

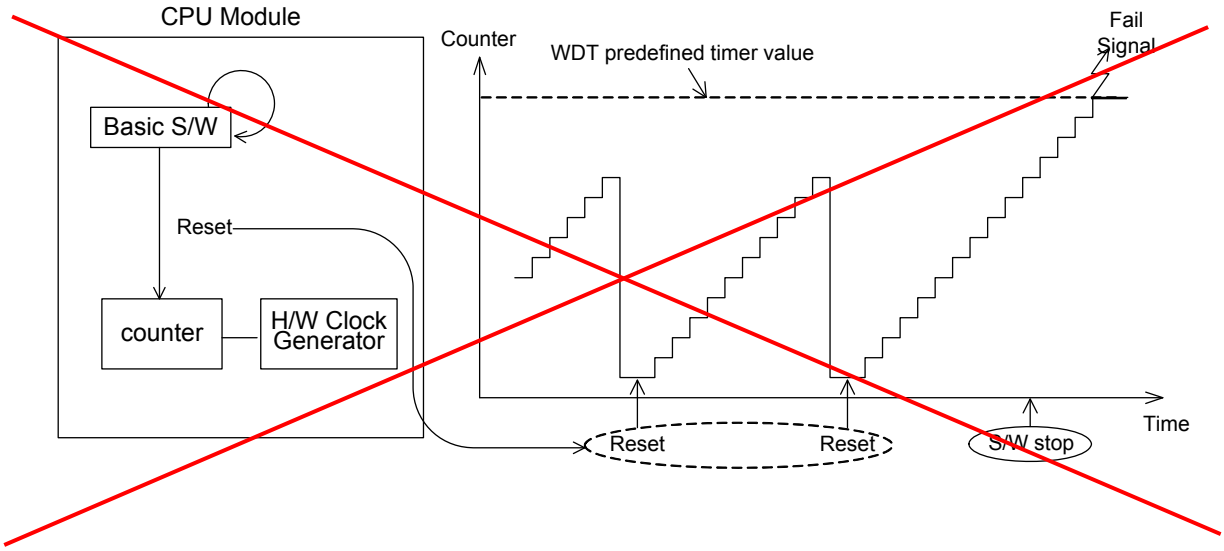
4.1.5.7.1.1 Function of the WDT

Figure 4.1-18 shows the architecture of the WDTs in MELTAC modules, and Figure 4.1-19 shows the WDT count-up, counter reset, and timeout behavior when the counter value reaches a predefined value.

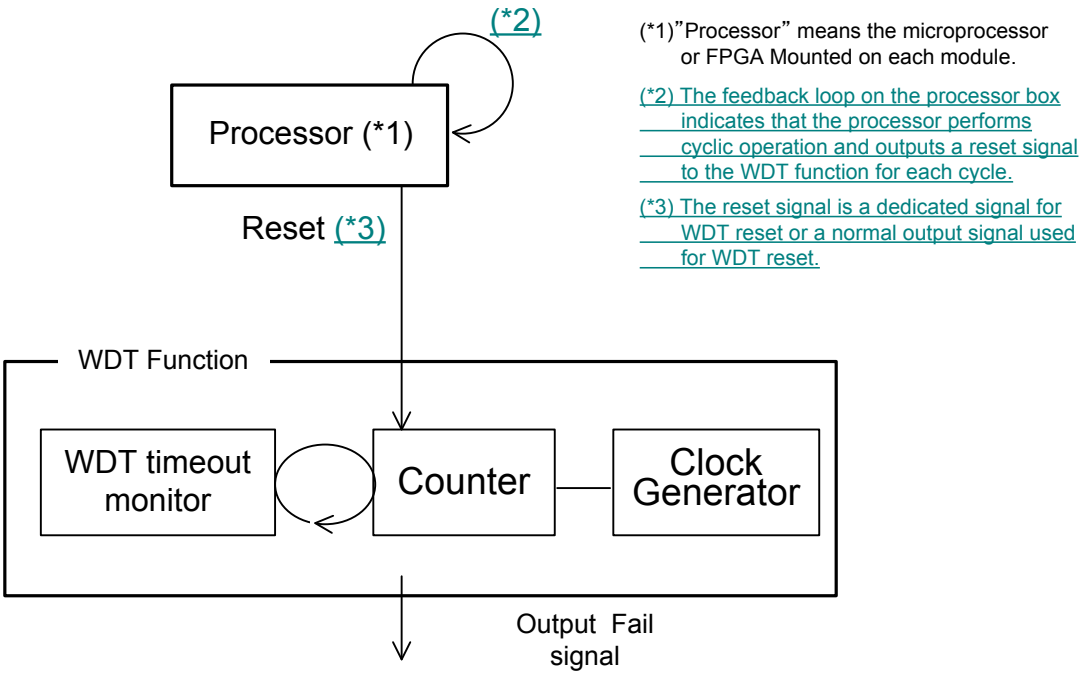
DCD_07.01-46
DCD_07.01-46 S01

(1)The WDT consists of a counter~~ with a hardware clock generator, and predefined timer value (for WDT timeout)~~, a WDT timeout monitor, and a clock generator, which are independent of the processor which executes safety functions. (See Figure 4.1-18) The WDT is both mounted on a device and applies a software architecture which is different from the microprocessor in the CPU Module that performs safety functions.

DCD_07.01-46
DCD_07.01-46 S01



DCD_07.01-46



DCD_07.01-46

DCD_07.01-46 S01

Figure 4.1-18 ~~Mechanism of WDT (CPU Module)~~WDT Architecture of MELTAC

(2)After initialization, the timer starts to count up. (See Figure 4.1-19)

(3)The WDT maintains normal operation through monitoring of the counter status to confirm that the counter value is periodically (i.e. for each operation cycle) reset by the processor. ~~The basic software resets the timer to zero at regular intervals (i.e. for each operation cycle).~~(See Figure 4.1-19)

DCD_07.01-46

(4)If the ~~basic software~~processor does not reset the ~~WDT~~ counter value within a predefined timer value, ~~then~~ a WDT timeout occurs. ~~the WDT times out and the controller transitions to a Failure mode(see Section 4.1.5) with an alarm indication.~~ The independence between the safety functions and the WDT functions is credited for separated modules.

DCD_07.01-46 S01

[

DCD_07.01-46

DCD_07.01-46 S01

Figure 4.1-19 Behavior of the WDT

DCD_07.01-46

DCD_07.01-46

DCD_07.01-46 S01

]

4.1.5.7.1.2 Behavior of safety function operation after WDT timeout

[

DCD_07.01-46 S01

DCD_07.01-46

DCD_07.01-46 S01

DCD_07.01-46 S01

]

DCD_07.01-46

DCD_07.01-46 S01

Figure 4.1-20 Behavior of the DO Module after CPU Module WDT timeout

[

DCD_07.
01-46 S01

DCD_07.
01-46

DCD_07.
01-46 S01

DCD_07.
01-46 S01

]

DCD_07.01-46

DCD_07.01-46 S01

Figure 4.1-21 Behavior of the other division's controller after the CPU Module WDT timeout

4.1.5.7.2 WDT Timeout Process (per Module)

[

DCD_07.01-46

DCD_07.01-46

DCD_07.01-46 S01

DCD_07.01-46

DCD_07.01-46

DCD_07.01-46 S01

DCD_07.01-46

DCD_07.
01-46

]

DCD_07.
01-46

DCD_07.
01-46 S01

DCD_07.
01-46

Figure 4.1-22~~19~~ WDTs Mounted in MELTAC Platform

DCD_07.
01-46

[

DCD_07.
01-46

DCD_07.
01-46 S01

DCD_07.
01-46

DCD_07.
01-46

DCD_07.
01-46

DCD_07.
01-46

DCD_07.
01-46

DCD_07.
01-46 S01

DCD_07.
01-46

DCD_07.
01-46

DCD_07.
01-46 S01

DCD_07.
01-46

DCD_07.
01-46 S01

]

Table 4.1-6 WDT Timeout Process (1/3)

Mod	Timeout occurrence part	Transition of a~~own~~ controller	Process signal output	No	Communication path to other controllers	Information passed to other controllers	How it is ~~shown~~seen from other controllers

DCD_07.01-46

Table 4.1-6 WDT Timeout Process (2/3)

Mod	Timeout occurrence part	Transition of a~~own~~ controller	Process signal output	No	Communication path to other controllers	Information passed to other controllers	How it is ~~shown~~seen from other controllers

DCD_07.01-46

Table 4.1-6 WDT Timeout Process (3/3)

Mod	Timeout occurrence part	Transition of a~~own~~ controller	Process signal output	No	Communication path to other controllers	Information passed to other controllers	How it is ~~shown~~seen from other controllers

DCD_07.01-46

6.1.8 Software Installation

[

DCD_07.01-46 S01

]

E.2.2 Analysis of Self-Diagnosis Functions

The results of analyzing the self-diagnosis functions are as follows.
In the “Description of diagnosis” column of each table, if it is described that the MELTAC platform (the CPU Module) transitions to ~~f~~Failure mode, platform functions cannot be continued, and the fault is identified as a potential hazard.
If the MELTAC platform transitions to any modes other than ~~f~~Failure mode or if it does not perform a transition (there is no description of mode transition), platform functions are not interfered with by the fault, and the fault is identified as a mitigable fault.

DCD_07.01-46 S01

E.2.2.1 CPU Module

Table E.2-2A CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-2B CPU Module

DCD_07.01-46 S01

DCD_07.09-27 S01

Table E.2-2C CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-2D CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-2E CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-2F CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-2G CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.2 System Management Module (SMM)

Table E.2-3A System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-3B System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-3C System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-3D System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-3E System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-3F System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.3 Bus Master Module

Table E.2-4A Bus Master Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-4B Bus Master Module

DCD_07.01-46 S01

DCD_07.09-27 S01

Table E.2-4C Bus Master Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-4D Bus Master Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-4E Bus Master Module

DCD_07.01-46 S01

E.2.2.4 Control Network I/F Module

Table E.2-5A Control Network I/F Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-5B Control Network I/F Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-5C Control Network I/F Module

DCD_07.01-46 S01

Table E.2-5D Control Network I/F Module

DCD_07.01-46 S01

DCD_07.09-27 S01

Table E.2-5E Control Network I/F Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-5F Control Network I/F Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.5 FMU Module

Table E.2-6A FMU Module

DCD_07.01-46 S01

DCD_07.09-27 S01

Table E.2-6B FMU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-6C FMU Module

Table E.2-~~7A~~6D ~~Touch Panel Interface~~ FMU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

~~Table E.2 7B Touch Panel Interface Module~~

DCD_07.01-46 S01

DCD_07.01-46 S01

E.2.2.6 ~~Touch Panel Interface Module~~ This section intentionally left blank

E.2.2.7 Safety VDU Panel

Table E.2-~~8~~7 Safety VDU Panel

DCD_07.01-46 S01

E.2.2.8 Analog Input Module

Table E.2-~~9~~8A Analog Input Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-~~9~~8B Analog Input Module

DCD_07.01-46 S01

E.2.2.9 Analog Output Module

DCD_07.01-46 S01

DCD_07.09-27 S01

Table E.2-~~10~~9A Analog Output Module

Table E.2-~~10~~9B Analog Output Module

DCD_07.01-46 S01

Table E.2-9C Analog Output Module

DCD_07.01-46 S01

DCD_07.01-46 S01

E.2.2.10 Digital Input Module

Table E.2-~~11~~10A Digital Input Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-10B Digital Input Module

DCD_07.01-46 S01

DCD_07.09-27 S01

E.2.2.11 Digital Output Module

Table E.2-~~12~~11A Digital Output Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-11B Digital Output Module

DCD_07.01-46 S01

DCD_07.01-46 S01

DCD_07.01-46 S01

DCD_07.01-46 S01

DCD_07.01-46 S01

E.2.2.12 PIF Module

Table E.2-~~13~~12A PIF Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-~~13~~12B PIF Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.13 Repeater Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-~~14~~13 Repeater Module

E.2.2.14 Power Supply Module

Table E.2-~~15~~14 Power Supply Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.15 Controller Cabinet

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-~~16~~15 Controller Cabinet

E.2.2.16 Others

Table E.2-16A Others

DCD_07.01-46 S01

DCD_07.01-46 S01

Table E.2-16B Others

DCD_07.01-46 S01

Table E.2-16C Others

Table E.2-16D Others

DCD_07.01-46 S01

Table E.2-16E Others

DCD_07.01-46 S01

E.2.3 Analysis of Communication Functions （Detectability of External Communication Data Faults）

The results obtained from analyzing the detectability of external communication data faults are described in “MELTAC Platform ISG-04 Conformance Analysis” (MUAP-13018).
The sections that provide analysis for each fault in MUAP-13018 are as listed in the Analysis Columns of the Table below.

As described in the analysis of MUAP-13018, the MELTAC platform will not transition to ~~f~~Failure mode due to any external communication data faults shown in the table below. Thus the external communication data faults below are all identified as mitigable faults. DCD_07.01-46 S01

Table E.2-17 Detectability of External Communication Data Faults

Analysis:

DCD_07.01-46 S01

Security-Related Information -Withheld Under 10CFR2.390