MITSUBISHI HEAVY INDUSTRIES, LTD.

1-1, WADASAKI-CHO, 1-CHOME, HYOGO-KU,
KOBE, 652-8585 JAPAN

April 25, 2014

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Attention: Mr. Perry Buckberg

Docket No. 52-021
MHI Ref: UAP-HF-14040

Subject: MHI's Response to US-APWR DCD RAI No. 1094-7466 (SRP 07.01)

Reference: 1) "Request for Additional Information No. 1094-7466, SRP Section 07.01 – Instrumentation and Controls – Introduction - Application Section: 7.1," dated March 27, 2014.

With this letter, Mitsubishi Heavy Industries, Ltd. (MHI) transmits to the U.S. Nuclear Regulatory Commission (NRC) a document entitled "Response to US-APWR DCD RAI No. 1094-7466 (SRP 07.01)."

Enclosed are the responses to the questions contained within Reference 1.

As indicated in the enclosed materials, this document contains information that MHI considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential. A non-proprietary version of the document is also being submitted with the information identified as proprietary redacted and replaced by the designation "[ ]."

This letter includes a copy of the proprietary version of the RAI response (Enclosure 2), a copy of the non-proprietary version of the RAI response (Enclosure 3), and the Affidavit of Atsushi Kumaki (Enclosure 1) which identifies the reasons MHI respectfully requests that all material designated as proprietary in Enclosure 2 be withheld from disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

Please contact Mr. Joseph Tapia, General Manager of Regulatory Services, Mitsubishi Nuclear Energy Systems, Inc. if the NRC has questions concerning any aspect of this submittal. His contact information is provided below.

D081
NRO

Sincerely,

Atsushi Kumaki,
Manager, APWR Project Group
Global Nuclear Project Department
Nuclear Energy Systems Division
Energy & Environment Domain
Mitsubishi Heavy Industries, Ltd.

Enclosures:

1. Affidavit of Atsushi Kumaki

2. Response to US-APWR DCD RAI No. 1094-7466 (SRP 07.01)
   (Proprietary)

3. Response to US-APWR DCD RAI No. 1094-7466 (SRP 07.01)
   (Non-Proprietary)

CC: P. Buckberg
J. Tapia

Contact Information
Joseph Tapia, General Manager of Regulatory Services
Mitsubishi Nuclear Energy Systems, Inc.
11405 North Community House Road, Suite 300
Charlotte, NC 28277
E-mail: joseph_tapia@mnes-us.com
Telephone: (704) 945-2740

ENCLOSURE 1

Docket No. 52-021
MHI Ref: UAP-HF-14040

MITSUBISHI HEAVY INDUSTRIES, LTD.
AFFIDAVIT

I, Atsushi Kumaki, being duly sworn according to law, depose and state as follows:

1. I am Manager, APWR Project Group, Global Nuclear Project Department, Nuclear Energy Systems Division, Energy & Environment Domain, Mitsubishi Heavy Industries, Ltd.(MHI) and have been delegated the function of reviewing MHI 's US-APWR documentation to determine whether it contains information that should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

2. In accordance with my responsibilities, I have reviewed the enclosed document entitled "Response to US-APWR DCD RAI No. 1094-7466 (SRP 07.01)," dated April, 2014 and have determined that the document contains proprietary information that should be withheld from public disclosure. Those pages containing proprietary information are identified with the label "Proprietary" on the top of the page and the proprietary information has been bracketed with an open and closed bracket as shown here "[ ]." The first page of the document indicates that information identified as "Proprietary" should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

3. The information identified as proprietary in the enclosed document has in the past been, and will continue to be, held in confidence by MHI and its disclosure outside the company is limited to regulatory bodies, customers and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and is always subject to suitable measures to protect it from unauthorized use or disclosure.

4. The basis for holding the referenced information confidential is that it describes the unique design and methodology developed by MHI for the I&C design of the US-APWR.

5. The referenced information is being furnished to the Nuclear Regulatory Commission (NRC) in confidence and solely for the purpose of information to the NRC staff.

6. The referenced information is not available in public sources and could not be gathered readily from other publicly available information. Other than through the provisions in paragraph 3 above, MHI knows of no way the information could be lawfully acquired by organizations or individuals outside of MHI.

7. Public disclosure of the referenced information would assist competitors of MHI in their design of new nuclear power plants without incurring the costs or risks associated with the design and testing of the subject systems. Therefore, disclosure of the information contained in the referenced document would have the following negative impacts on the competitive position of MHI in the U.S. nuclear plant market:

   A. Loss of competitive advantage due to the costs associated with development of the safety I&C system. Providing public access to such information permits competitors to duplicate or mimic the safety I&C system design without incurring the associated costs.

B. Loss of competitive advantage of the US-APWR created by benefits of enhanced plant safety, and reduced operation and maintenance costs associated with the safety I&C system.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information, and belief.

Executed on this 25th day of April, 2014.

Atsushi Kumaki,
Manager, APWR Project Group
Global Nuclear Project Department
Nuclear Energy Systems Division
Energy & Environment Domain
Mitsubishi Heavy Industries, Ltd.

Docket No. 52-021
MHI Ref: UAP-HF-14040

Enclosure 3

Docket No. 52-021
UAP-HF-14040

Response to US-APWR DCD RAI No. 1094-7466 (SRP 07.01)

April 2014

(Non-Proprietary)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/23/2014

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.:	**1094-7466**
SRP SECTION:	**07.01 – Instrumentation and Controls – Introduction**
APPLICATION SECTION:	**07.01 – Instrumentation and Controls – Introduction**
DATE OF RAI ISSUE:	**3/27/2014**

QUESTION NO.: 07.01-46

On December 5, 2013, Mitsubishi Nuclear Energy Services, Inc. (MNES) and NRC Staff presented the US-APWR Design Certification Document (DCD), Chapter 7, Instrumentation and Controls, and the staff's Phase 2 Safety Evaluation with Open Items to the Full Committee of the Advisory Committee on Reactor Safeguards (ACRS). In its letter to the Executive Director for Operations (EDO) dated December 24, 2013, the ACRS made the following comment regarding Chapter 7 (ML13346A732).

> The staff should ensure that sufficient design information is available to provide assurance that watchdog timers will produce the desired reactor protection and engineered safety features actuation failure state signals independently from the Mitsubishi Electric Total Advanced Controller (MELTAC) platform software.

Additional information in support of the comment was provided in the body of the letter. On February 24, 2014, the EDO responded to the ACRS (ML13365A056). That response provided the staff's view that the WDT timers will produce the desired actuation failure state signals independently from the MELTAC platform software. However, staff acknowledged that docketed information may need additional clarification to better reflect this aspect of WDT operation. It further stated that NRC staff would work with the applicant to address this issue.

Staff has completed its review of the docketed information, including the DCD and referenced technical reports, attempting to identify locations where the existing descriptions of WDT operations could be further clarified.

Staff requests the applicant to review the following sections of MUAP-07005, revision 9, "Safety System Digital Platform - MELTAC-" for clarification as identified in the table below.

Section 4.1.5 Self-Diagnosis, (pg 61) "The MELTAC platform controller is equipped with the three types of self-diagnosis features: a hardware based detection process, a software based detection process and a combination thereof."	This section does not provide enough information and detail to determine whether the hardware diagnosis circuitry which involves watchdog timer is independent of the software based detection process. Additional detail and clarification is needed.
Section 4.1.5, 1) Failure, [ ]	[ ]
Section 4.1.5.2.1 CPU Module [ ]	[ ]
Section 4.1.5.2.1 CPU Module [ ]	[ ]
Section 4.1.5.2.1 CPU Module [ ]	[ ]
Section 4.1.5.2.1 CPU Module [ ]	[ ]

Section 4.1.5.5.2 Output Module [ ]	[ ]
Figure 4.1-18, **Mechanism of WDT (CPU Module)** Figure depicts a graphical representation of the WDT mechanism; however, it does not represent detailed interactions of the WDT circuitry to the circuitry involving the platform software.	Detailed graphical depiction is needed to determine any dependencies arising from the interactions of the WDT circuitry and the platform software.
Figure 4.1-19, **WDT's Mounted in MELTAC Platform** [ ]	[ ]

ANSWER:

Independence of Watchdog Timers (WDTs) function

The watchdog timer (WDT) consists of a hardware counter, a hardware clock generator, and a hardware WDT timeout monitor, which includes a predefined timer value for WDT timeout. The hardware circuits of the WDT are independent from the software (both basic and application) and the processing system hardware circuits which execute the software of the MELTAC controller that performs the safety functions. After initialization of the software of the MELTAC controller, the hardware counter of the WDT starts to count up automatically by hardware circuits.

[

]

As explained above, the WDT actuation mechanism and the MELTAC controller's response after detecting the WDT timeout are independent from the software and hardware circuits of the MELTAC controller that performs the safety functions.

Behavior of safety I&C systems after detection of WDT timeout
[

]
As explained above, the mechanism of WDT actuation and the behavior of MELTAC controllers after detecting a WDT timeout are independent from the software and hardware circuits of the MELTAC controllers that perform safety functions.

MHI agrees with the NRC staff request to add detail and clear descriptions on the WDT as described in Table-1.

To respond to the comments and requests from the ACRS and the NRC staff, MHI will add descriptions of the independence between the WDT and the software and hardware circuits of the MELTAC controller that perform safety functions to DCD Tier 2 Chapter 7 and MUAP-07005 as shown in Attachments 1 and 2.

Table-1: Answer to the NRC staff requests to resolve the WDT issue

References to MUAP-07005, revision 9

Section 4.1.5 Self-Diagnosis, (pg 61) "The MELTAC platform controller is equipped with the three types of self-diagnosis features: a hardware based detection process, a software based detection process and a combination thereof."	**NRC Staff Request** This section does not provide enough information and detail to determine whether the hardware diagnosis circuitry which involves watchdog timer is independent of the software based detection process. Additional detail and clarification is needed. **MHI Answer** Summary descriptions of Subsection 4.1.5.7 will be added after the second paragraph of Subsection 4.1.5. Description on the WDT mechanism independence from the software will be added in Subsection 4.1.5-a).
Section 4.1.5, 1) Failure, [ ]	**NRC Staff Request** [ ] **MHI Answer** [ ]
Section 4.1.5.2.1 CPU Module [ ]	**NRC Staff Request** [ ] **MHI Answer** [ ]
Section 4.1.5.2.1 CPU Module [ ]	**NRC Staff Request** [ ] **MHI Answer** [ ]

Section 4.1.5.2.1 CPU Module [ ]	**NRC Staff Request** [ ] **MHI Answer** [ ]
Section 4.1.5.2.1 CPU Module [ ]	**NRC Staff Request** [ ] **MHI Answer** [ ]

Section 4.1.5.5.2 Output Module [ ]	**NRC Staff Request** [ ] **MHI Answer** [ ]
Figure 4.1-18, Mechanism of WDT (CPU Module) Figure depicts a graphical representation of the WDT mechanism; however, it does not represent detailed interactions of the WDT circuitry to the circuitry involving the platform software.	**NRC Staff Request** Detailed graphical depiction is needed to determine any dependencies arising from the interactions of the WDT circuitry and the platform software. **MHI Answer** MHI will add detailed graphical descriptions in Figure 4.1-18 and revise the description of Subsection 4.1.5.7 to explain the interactions of the WDT circuitry and the platform software.
Figure 4.1-19, WDT's Mounted in MELTAC Platform [ ]	**NRC Staff Request** [ ] **MHI Answer** [ ]

Impact on DCD
Descriptions for the independence between the WDT and the software and hardware circuits of the MELTAC controller that performs the safety functions have been added to DCD Tier 2, Section 7.1, as shown in Attachment-1.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on PRA
There is no impact on the PRA.

Impact on Technical / Topical Report
Descriptions for the independence between the WDT and the software and hardware circuits of the MELTAC controller that performs the safety functions have been added to MUAP-07005, as shown in Attachment-2.

7.1.3.10 Self-Diagnosis Function

The integrity of digital I&C components is continuously checked by their self-diagnostic features which consist of software based detection functions and hardware based detection circuits (watchdog timers [WDTs]). These self-diagnostic features result in early detection of failures and allow on-line repair that improves system availability. Information about detected failures is gathered through networks and provided to maintenance staff in a comprehensive manner. ~~In addition, the self-diagnostic features control~~ If any failures that disable safety functions are detected by these self-diagnostic features, alarms are generated in the MCR and safety-related signals are forced into a predetermined safe status, such as, "fail-safe" for reactor trip signals and "fail as-is" for the ESF actuation signals as shown in Figure 7.1-8. Lower priority alarms are generated in the MCR for other failures that do not disable the safety functions, such as a failure of one controller in a parallel redundant pair; where a redundant controller configuration~~, to maintain all system functions,~~ is employed to maintain all system functions even in the presence of failures. The self-diagnosis is always working in the digital control system but does not affect system operation. Therefore, there is no impact to channel independence, system integrity and compliance to the single failure criterion during self-testing.

MIC-04-07-00001
DCD_07.01-46
MIC-04-07-00001

There are numerous self-diagnostic functions and WDT functions within the different modules of the MELTAC digital platform. Each WDT is continuously reset (avoiding timeout) based on the cyclical execution of the module's function. A WDT time out occurs when the cyclical execution is interrupted, indicating a failure. The WDT consists of a hardware counter, a hardware clock generator, and a hardware WDT timeout monitor, which includes a predefined timer value for WDT timeout. The hardware circuits of the WDT are independent from the software (both basic and application) and the processing system hardware circuits which execute the software of the MELTAC controller that performs the safety functions. A WDT timeout within one module is detected by another module in the same controller or in another controller through loss of data communication with the failed module. This other module/controller then generates an alarm signal for the failure. The details of the self-diagnostic functions and the WDTs are described in MUAP-07005 Subsection 4.1.5.

MIC-04-07-00001
DCD_07.01-46

Continuous self-diagnostic features allow elimination of most of the manual surveillance testing required for technical specification compliance. Manual testing and manual calibration verification are specifically provided for functions with no self-diagnosis. The integrity of the self-diagnosis is confirmed by a periodic manually initiated memory integrity check, which includes the software memory which is used for self-diagnosis. For PSMS, this software memory check requires temporarily connecting each PSMS controller to the Maintenance Network. When a PSMS controller is connected to the Maintenance Network, it is considered inoperable. The functions affected by an inoperable controller are managed by plant technical specifications. PCMS controllers are permanently connected to the Maintenance Network.

In addition, when I/O is checked by manual sensor calibration and output actuation of plant components, the digital components which are self-tested are also re-checked. This provides manual confirmation for the integrity of all digital functions. The coverage of self-diagnosis and manual test is described in MUAP-07004 Sections 4.3 and 4.4. MUAP-07005 Subsection 4.1.5.1 describes self-diagnosis. The self-testing is provided for

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 watchdog timer architecture and error detection process (including the behavior after error detection) of the MELTAC platform is described in Section 4.1.5.7. The watchdog timer consists of hardware circuitry and operates independent of software (basic and application). DCD_07.01-46

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, parity error, timeout, analog input check, etc.
The diagnosis of these features is performed by hardware circuitry, which is independent of software (basic and application). DCD_07.01-46

b) Software based detection process

With this feature, self-diagnosis is implemented using software. The feature involves CPU healthy check, ROM error check, RAM error check, etc.

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 presetspecified and a predetermined failure mode output value set on the output module during the loading of the application software to MELTAC Platformat the application level. See 4.1.5.5.2.b for details.

DCD_07 .01-46

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.
In case of redundant standby controller configuration, when the I/O Alarm occurs in the Redundant I/O in the Control Mode, the subsystem stops to use this I/O, switches the other I/O from the Standby mode to the Control Mode, and continues the processing of input/output.

4.1.5.1 Coverage of Self-diagnosis

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

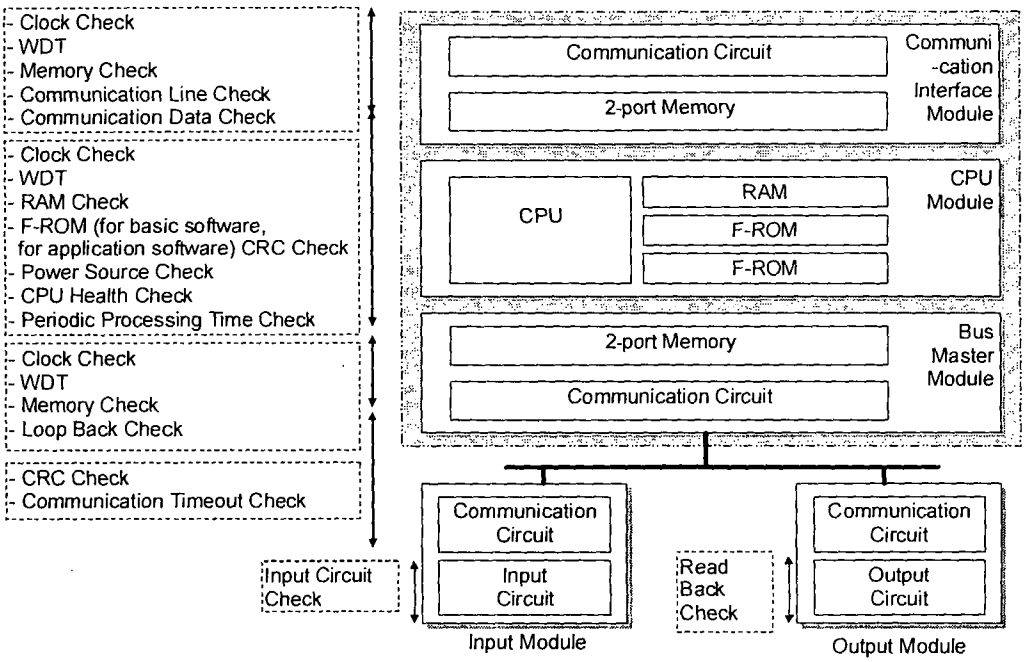


Figure 4.1-17 Coverage of Self-Diagnosis Function of the Controller

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

4.1.5.2.1 CPU Module

[

DCD_07
.01-46

DCD_07
.01-46

]

[

DCD_07
.01-46

]

[

DCD_07
.01-46

]

[

]

4.1.5.5.2 Output Module

[

DCD_07
.01-46

DCD_07
.01-46

]

4.1.5.5.3 Controller Cabinet

[

]

4.1.5.6 Operations When the Hardware and Software Do Not Match

Mismatch of the module configuration in the CPU chassis:
The CPU Module detects the error and the subsystem turns to Failure mode.

Mismatch of the module configuration in the I/O chassis:
The CPU Module detects the mismatch and notifies the application software logic that the I/O signals have bad quality, as explained in Section 4.1.5.

4.1.5.7 Watchdog Timer (WDT)

This section provides a description of the WDT architecture and how WDT timeouterrors is processed in the MELTAC modules. [ ] DCD_07.01-46

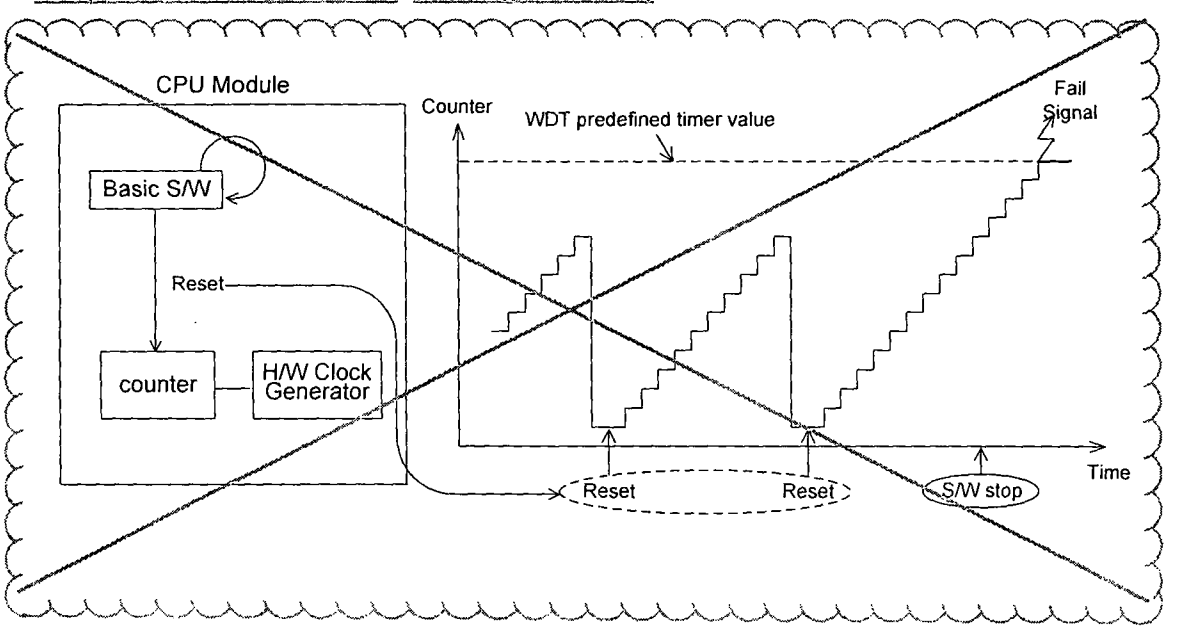
4.1.5.7.1 Architecture of the WDT

~~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:
(a) Function of the WDT
(b) Behavior of safety function operation after detection of WDT timeout

(a) Function of the WDT
Figure 4.1-18 shows the arrangement of the WDT in the CPU Module, and Figure 4.1-19 shows how the WDT operates regarding count-up, counter reset, and timeout when the counter value reaches a predefined value. The sequence of WDT operation in the event of a failed module is discussed below. A failure in the CPU Module has been used as an example; the operation of the WDT in other modules is identical.

(1)The WDT consists of a counter with a hardware clock generator, and predefined timer value (for WDT timeout) which are independent from the MELTAC basic software and the processing system hardware circuits which execute the software of the MELTAC controller that performs safety functions. (See Figure 4.1-18) DCD_07.01-46



DCD_07
.01-46

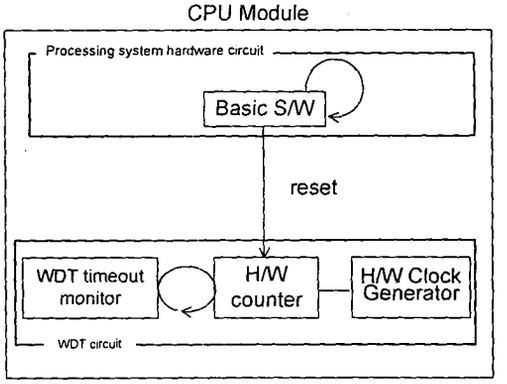


Figure 4.1-18 ~~Mechanism of WDT (CPU Module)~~WDT Feature (CPU Module)

(2)After initialization, the timer starts to count up approaching the WDT's predefined timeout value, which is preset in the WDT H/W.(See Figure 4.1-19)

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

(4)If the basic software does not reset the~~WDT~~ counter value within a predefined timer value, then a WDT timeout occurs and is detected by hardware. ~~the WDT times out and the controller transitions to a Failure mode(see Section 4.1.5) with an alarm indication.~~

[

]

DCD_07
.01-46

Figure 4.1-19 Behavior of WDT (CPU Module)

~~The mechanism of other modules is the same as that of the CPU Module.~~

[

DCD_07
.01-46

]

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

DCD_07
.01-46

[

]

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

4.1.5.7.2 WDT Timeout Process (per Module)

[

DCD_07
.01-46

DCD_07
.01-46

]

DCD_07.01-46

DCD_07.01-46

DCD_07.01-46

Figure 4.1-2219 WDTs Mounted in MELTAC Platform

[

DCD_ 07.01-46

DCD_ 07.01-46

DCD_ 07.01-46

DCD_ 07.01-46

DCD_ 07.01-46

DCD_ 07.01-46

DCD_ 07.01-46

DCD_ 07.01-46

DCD_ 07.01-46

]

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