**Module -- WdgM**

[1 References 2](#_Toc337038442)

[2 Configuration Settings 2](#_Toc337038443)

[2.1 Naming Conventions 2](#_Toc337038444)

[2.2 Graphical Node Map Generation 2](#_Toc337038445)

[3 Known Issues / Limitations With Configuration 3](#_Toc337038447)

[4 Integration 4](#_Toc337038448)

[5 Revision Control Log 4](#_Toc337038449)

# References

1. Safe Watchdog Manager User Manual v1.7.0 (S-WdgM \_UserManual.pdf)
2. Real-Time Interrupt (RTI) Module SPNUxxx-May 2011 (RTI\_Gladiator.pdf)
3. **TBD** – Placeholder for safety requirements dictating division of application software

# Configuration Settings

## Naming Conventions

Naming conventions are used in the configuration of the module to:

1. Allow easy identification of the Local Transition and Global Transition configuration containers when configuring the BSW in Configurator
2. Provide an unambiguous link to the intended SWC Checkpoint to which the resulting generated port will be mapped. This convention facilitates:
   1. Usage of the “Auto Map Service Ports” mapping feature in DaVinci Configurator after importing the generated WdgM SWC description.
   2. Generation of an intuitive graphical view of the configuration via GraphViz (i.e. the nodes of the graph are labeled with the Checkpoint container names).

|  |  |  |
| --- | --- | --- |
| **Element** | **Convention** | **Example** |
| Supervised Entity | SE<Entity Short Name> | SE2msA |
| Local Transition | LT\_<##> | LT\_01  Note that contiguous numbering is not required. Due to deletion of vectors, the number may become discontinuous. |
| Global Transition | GT\_<##> | GT\_01  Note that contiguous numbering is not required. Due to deletion of vectors, the number may become discontinuous. |
|  |  |  |

## Graphical Node Map Generation

Nexteer has extended the delivered generator to include generation of a graphical node map of the configuration. As there is no “comfort” view available for configuration, the task of visualizing the resultant configuration based on the numerous configuration containers is impossible except in extremely simple configurations.

The graphical node map generation relies on the Artt framework and GrapViz open source engine. Artt is included in the integration projects, however the installation of GraphViz and inclusion of the GraphViz utility on the system PATH variable must be performed by the developer on his/her local computer. GraphViz is available for download from <http://www.graphviz.org/>.

The graphical output, WdgM\_Graph.pdf, is generated in the folder along with the generated .h/.c files. Note that Adobe PDF reader locks any file that it has open from being modified, so if the WdgM\_Graph.pdf is open in Adobe PDF reader and the generation process is run, the generation will fail. A solution to this issue is to download a PDF viewer that does not lock the file while it is opened (e.g. SumatraPDF).

## Configuration Selection Rationale

The configuration of the WdgM is intended to meet the requirements defined in [3].

### Deadline Monitoring

WdgM Deadline monitoring is not used to meet any of the requirements. As understood by the software team, the use of the WdgM deadline monitoring is not necessary to provide the “Deadline” monitoring defined in the requirements.

Deadline monitoring has the following limitations:

1. Deadlines are defined as the time to perform a single transition
2. The deadline is only evaluated if the associated transition is taken (i.e. if the initial checkpoint of the deadline monitored transition has multiple outgoing transitions, then in order for the deadline to be evaluated, the destination checkpoint of the deadline monitored transition must be executed before any of the other outgoing transition destination checkpoints.)
   1. For the Nexteer EPS use case where the requirements define a “deadline” over an entire task chain:
      1. Either the deadline monitored transition would need to be defined as a separate set of checkpoints to the checkpoints used for monitoring local/global task transitions.
      2. Or the initial and final checkpoints of a task chain would need to be excluded from the local transition monitoring and used only for “deadline” monitoring.
3. A deadline is only evaluated when the destination checkpoint of the transition is reached (i.e. there is not cyclic check on the checkpoint time to detect when the deadline time has been exceeded, yet the destination checkpoint has not yet been reached.)
   1. This means that a task that fails to activate will not be detected by deadline monitoring. Example failures are a task never finishing because of an infinite loop within the task or failure of the Os alarm operation for the task.
   2. Although the requirements defined in [3] do not contain an explicit requirement for monitoring the cyclic execution of a set of checkpoints (i.e. execution frequency), verbal conversations with the FDD authors have provided the software team with the understanding that the intent of the “Deadline” requirement is to provide a monitoring solution that detects when the frequency of given checkpoint series has a period that is greater than the “Deadline” threshold stated. Additionally, the software group assumes that a frequency of execution that produces a period less than the “Deadline” threshold is desired to be detected. For this purpose, the software group has determined that Alive monitoring is the most straightforward method to provide the required monitoring/failure detection.

### Alive Monitoring

Alive monitoring is used to meet the “Deadline” monitoring specified in the requirements. The concept of “Deadline” monitoring defined in the requirements shall be referred to as “Alive monitoring” from here forward to prevent confusion with the WdgM deadline monitoring.

Alive monitoring is performed by the WdgM\_Mainfunction which is scheduled in a 4ms alarm activated task. The 4ms cyclic rate was selected to be less than the required system fail action time of 16ms(TBC), provide appropriate resolution for configured WdgM monitoring, and minimize the CPU throughput required.

Alive monitoring has the following limitations:

1. The cycle period measurement has a precision of the WdgM\_Mainfunction call.
   1. Due to a 4ms monitoring period the following non-optimal compromises were made.
      1. The monitoring cycle of the 2ms task chain is 4ms with an expected 2 alive indications. This is deemed acceptable because…TBD
      2. The monitoring cycle for the 10ms task chain is 40 ms with and expected 2 alive indications. This is deemed acceptable because…TBD
2. The WdgM monitoring period begins with the first call of the WdgM\_Mainfunction, direct synchronization with the Alive monitor checkpoint is not provided.
   1. Since all task alarms being monitored are started synchronously with the WdgM task alarm and all have a 0 tick offset, then the “cycle period monitored” by the WdgM main function for Alive monitoring will start synchronously with the alarm expirations. Given this, then the task execution jitter causing one monitor period to detect 2 alive monitor indications and the next period to detect 0 alive monitor indications is not a scenario that needs to be considered as valid (i.e. detecting this scenario as a failure meets the requirements).
3. An initial checkpoint can be executed multiple times without causing a program violation. Given this, then placing the alive monitoring at a checkpoint that can only be executed once without violation detection is desired. The last checkpoint in the Task chain is selected for consistency.

### Local Transition Monitoring

### WdgMMode

|  |  |  |
| --- | --- | --- |
| **Attribute Name** | **Value** | **Rationale** |
| WdgMExpiredSupervisionCycleTol | 0 | The EPS use case does not require a delay after failure detection to perform processing prior to activating the failure reaction, therefore, 0 is selected to perform the fail action in the same WdgM\_Mainfunction call that confirms a failure exists. |
| WdgMModeId | 0 | This is the only mode configured, so it is the first Id value, 0. |
| WdgMTicksPerSecond | 1000000 | TBC. Although the deadline monitoring feature which uses this timer is not configured, and the requirements in [3] are not clear on the accuracy of time measurement required, it is assumed by the software team that a resolution of 1uS is sufficient. |
| WdgMSupervisionCycle | 0.004 | The WdgM\_Mainfunction is scheduled at 4ms, see rationale stated earlier in this document for selection of 4ms. |
| WdgMInitialTriggerModeId | 0 | 0 is the Id of the WdgMTrigger definition which triggers the TMS570 Hardware DWWD. This is the only defined WdgMTrigger and therefore must be the initial trigger mode. |
| WdgMLocalStatusParams\_SE0 | | |
| WdgMFailedSupervisionRefCycleTol | 0 | [3] requires no tolerance for alive failures. Per [1] §4.4.2, 0 accomplishes the required functionality. |
| WdgMSupervisedEntityInitialMode | WDGM\_LOCAL\_STATUS\_OK | TBD |
| WdgMFailedDeadlineRefCycleTol | 0 | [3] requires no tolerance for failures. Per [1] §4.1.9, 0 accomplishes the required functionality.  (note that deadline monitoring is unused in EPS system) |
| WdgMDeadlineReferenceCycle | 0 | [3] requires no tolerance for failures. Per [1] §4.1.9, 0 accomplishes the required functionality.  (note that deadline monitoring is unused in EPS system) |
| WdgMFailedProgramFlowRefCycleTol | 0 | [3] requires no tolerance for program flow failures. Per [1] §4.1.9, 0 accomplishes the required functionality. |
| WdgMProgramFlowReferenceCycle | 1 | Per [1] §4.1.9, 1 configures the WdgM to check the results of the program flow supervision at every MainFunction cycle. |
| WdgMLocalStatusSupervisedEntityRef | CntrlPath\_SE0 |  |
| WdgMTrigger | | |
| WdgMWatchdogMode | WDGIF\_SLOW\_MODE | TBD |
| WdgMTriggerConditionValue | 6 | TBD |
| WdgMTriggerWindowStart | 2 | TBD |
| WdgMTriggerModeId | 0 | This parameter is currently unused by the TTTech implementation per the “Hover over” note viewable in Configurator. |
| WdgMTriggerWatchdogRef | WdgMWatchdog | This a reference to the only configured watchdog in the EPS system. |

#### WdgMGeneral

|  |  |  |
| --- | --- | --- |
| **Attribute Name** | **Value** | **Rationale** |
| WdgMDevErrorDetect | False | Only needs to be enabled in debug builds for troubleshooting issues with the WdgM configuration and use. Disabled for release configuration to save ROM. |
| WdgMDemReport | False | The EPS use case has no need for this feature. Disabling to eliminate any additional safety analysis related to this feature being enabled. |
| WdgMImmediateReset | True | Enabled for EPS so that the BAD Key status would be present in the watchdog status register after reset, which is used to set the proper NTC. |
| WdgMOffModeEnabled | False | The EPS use case has no need for this feature. Disabling to eliminate any additional safety analysis related to this feature being enabled. |
| WdgMVersionInfoApi | False | The EPS use case has no need for “VersionInfoApi”. |
| WdgMDefensiveBehavior | True | TBD |
| WdgMUseRte | True | EPS uses the WdgM in the context of the RTE for checkpoint calls. |
| WdgMDemSupervisionReport | False | The EPS use case has no need for this feature. Disabling to eliminate any additional safety analysis related to this feature being enabled. |
| WdgMFirstAliveCounterReset | True | Required to prevent first execution of WdgM MainFunction from detecting a failure against alive supervisions that have a reference cycle of 1. |
| WdgMUseOsSuspendInterrupt | True | TBD |
| WdgMTimebaseSource | WDGM\_INTERNAL\_HARDWARE\_TICK | TBD |
| WdgMSecondResetPath | False | TBD |
| WdgMTickOverrunCorrection | True | TBD |
| WdgMEntityDeactivationEnabled | False | The EPS use case has no need for this feature. Disabling to eliminate any additional safety analysis related to this feature being enabled. |
| WdgMGlobalStateChangeCbk | none | No EPS use case for this notification |
| WdgMStateChangeNotification | False | No EPS use case for this notification |
| WdgMGlobalMemoryAppTaskRef | ASIL\_D | This is the only application configured in the project at this time. |
| WdgMCallerIds | | |
| WdgMCallerId | 0 | TBD |
| TO BE COMPLETED…. | | |
|  |  |  |

# Known Issues / Limitations With Configuration

1. None

# Revision Control Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item #** | **Rev #** | **Change Description** | **Date** | **Author Initials** |
| 1 | 1.0 | Initial Creation | 28FEB13 | JJW |