# SDD Review Document

## Summary

|  |  |
| --- | --- |
| **Date** | 02-Feb-2021 |
| **Effort** | 40 min. |
| **Room/Location** | GitHub |
| **Review Status** | Open |
| **Review name** | SDD\_SafetyManager.doc |
| **Method** | DC |
| **Release** |  |
| **Responsible** | Ruben Cocoletzi |
| **Project** | Door Control Module |
| **Reason of Review** | Initial Review |

## Comment List

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Reference** | **Comments / Actions** | **Classification (E)rror/Risk / (R)emark** | **Responsible person/Planned date for completion** | **Completion(Name/Date)** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| … |  |  |  |  |  |

## Check List

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Description | OK / NOK / NR | Comment | Responsible person /  Planned date for completion | Status |
| 1 | Does the design comply to the SW architecture? (interfaces, scheduling...) | OK |  |  |  |
| 2 | Are all requirements allocated to Desing elements? | OK |  |  |  |
| 3 | Are all operations described in an adequate detail and with the adequate notation? | OK |  |  |  |
| 4 | Is the coupling level between SW parts (internal or externals) reduced to the minimum?  Is the justification of all global data written in the design document? | OK |  |  |  |
| 5 | Is each data owned by one unit?  If a data is public (for read and/or for write operations), is its access made using a method provided by the owner?  (if a method is provided for read and write operations on the same pubilc data, the data has to be private) | OK |  |  |  |
| 6 | How are the variables initialized? If not initialized, is the reason explained? | OK |  |  |  |
| 7 | Is the mechanism to initialise the functionality (when needed) described?  (eg: function calls, data acquisition …) | OK |  |  |  |
| 8 | In case of global variable (shared or not shared) used in reentrance function (reentrance raised by an ISR), is there a mechanism to avoid data modification during its treatment? | OK |  |  |  |
| 9 | Are Tasks, ISRs and event notification function kept as short as possible? | OK |  |  |  |
| 10 | Is the state variable only used in one single module?  (If the state variable needs to be visible from another module (to be avoided), indicate it in the design and use the mechanism of read copy on that variable). | OK |  |  |  |
| 11 | Is the event memorization (ex: flag) consumed at the end of each reccurence of a state machine?  Otherwise, the risk is to use an obsolete event (ex: event memorization consumption conditionned by a state transition). | OK |  |  |  |
| 12 | In case of asynchronous reception of the same event by several objects (ex: state machine, C function called periodicly…), has each object its own memorization mechanism (ex: separate flags). | OK |  |  |  |