# Purpose

The purpose of this this document is to document a software safety classification in accordance with clause 4.3 "Software safety classification" in IEC 62304:2006+AMD1:2015 and other applicable regulations.

# Scope

This document is intended to assign a software safety class to the software system comprised in *<Name of Medical device>.*

# References

## General

### SSI-SOP-20, Software Development and Validation

### SSI-SOP-13, Risk Management

## Regulations and Standards

### IEC 62304:2006+AMD1:2015, Medical Device – Software Lifecycle Processes

### *FDA Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 11, 2015*

### *<Remove/Add regulations and standards as need. Ensure the standard year and version are specified, as applicable>*

# Software System Safety Classification

## Description of the System

*<Provide an overall description of the software system>*

## Review of relevant hazardous situations (use if required)

*<The starting point for the software safety classification is to identify relevant hazardous situations. Firstly, identify when a failure in the software can contribute to a hazardous situation. Secondly, look for risk control measures implemented by the software because the software inherits the risk it is supposed to mitigate.*

*Once the relevant hazardous situations are identified, they can be assessed to determine how they influence the classification.*

*For this assessment, it is essential to understand the concept of Po = P1 x P2. If you don't recognize it, you might want to look at this free video before proceeding. You can also read more about the concept in ISO 14971:2019, Annex C "Fundamental risk concepts", or get an in-depth understanding by taking the online course Introduction to software for medical devices and IEC 62304.*

*When determining an SSC, the likelihood of software failure shall be 100%. Software failure is part of P1, but more factors may come into play when determining the likelihood of a hazardous situation occurring. Consequently, Po can be expressed as follows:*

*Po = P1SW x P1Ext x P2*

*P1SW == 100% prior software risk management activities.*

*P1EXT == Conditions external to the software required to result in a hazardous situation.*

*P1Ext can be one or several external risk control measures. External risk control measures can be another software system but never within the software system under review.*

*Perhaps it seems unnecessary to perform a detailed assessment for high-risk devices because it will result in Class C anyway. However, by documenting an evaluation, you will help others understand where to find the safety-critical parts in your software system, which is helpful for future design and maintenance work.*

*To avoid overshooting the classification, please note that injury used in IEC 62304 is more narrowly defined compared to harm in ISO 14971.*

*Even though it is not recommended to duplicate information, copying selected parts from your risk assessment into this document may improve readability. Still, feel free to delete columns from the table below but make sure to keep enough information to allow traceability to your risk analysis, for example, unique risk identifiers.*

*For this section, you have two alternatives:*

*Alternative 1, if you only find non-injury related risks, choose this first alternative and remove alternative 2. Move ahead and conclude, in section 3, that the software system is a class A system.*

The risk assessment [2] has been reviewed for software-related risks that may lead to injury; no applicable hazardous situations were identified.

*Alternative 2, if you find any risk that may lead to injury, use the section below and remove alternative 1 above. Please note that the examples provided in the table are made-up examples to give you an idea of how to use the table.*

*For the "Po assessment" in the table below, it is usually highly beneficial to have colleagues with clinical knowledge involved in the discussions. You could even consider asking such a person to act as the formal reviewer of this document, especially when class C risks are deemed acceptable, resulting in class B or even class A.*

The risk assessment [2] has been reviewed for software-related hazardous situations resulting in the below list.

*Please remove the example text in the table below with relevant information applicable to your product.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Risk ID* | *Hazardous situation* | *External RCM available?* | *Po assessment*  *(Po = P1 x P2)* | *Acceptable?*  *[Yes / No]* | *Resulting classification*  *[A / B / C]* |
| *12* | *Lungs are exposed to harmful air pressure.* | *RCM-12: Overpressure valve in the airpath way prevents harmful pressure.* | *The RCM is efficient and provides a strong P1Ext preventing the software from causing injury.* | *Yes* | *A* |
| *23* | *Lungs are not supported by sufficient air pressure.* | *Not available.* | *The hazardous situation may not lead to harm (P2) to all exposed patients, but the risk is too high.* | *No* | *C* |
| *25* |  |  |  |  |  |
| *26* | *Healthy tissue is exposed to harmful radiation* | *Not available* | *If SW calculations are way off, clinical staff might be able to identify the problem (P2) and reduce the likelihood of harm. Still, this is not acceptable, given the random behaviour of software failure.* | *No* | *C* |
| *31* | *Moving parts resulting in crush injury* | *RCM-007*  *Mechanical stop limits the minimum gap.* | *P1Ext suffice to prevent serious injury (Class C). However, the minimum gap is still too small to exclude the risk of non-serious injury.* | *No* | *B* |

*<To determine the Level of Concern per the FDA software classification, Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices shall be used (Table 1 and 2)*

*e.g. Table 1: a device is of Major level of concern if “Prior to mitigation of hazards, could a failure of the Software Device result in death or serious injury, either to a patient or to a user of the device?”.*

*Table 2: A device is of Major level of concern if “Prior to mitigation of hazards, could a failure of the Software Device result in death or serious injury, either to a patient or to a user of the device?”.*

*The FDA required that rationale for the decision is documented and decision-making process is evident in the provided documentation>*

## Safety Classification

**Safety Class According to IEC 62304:**

| ***System/Item/Unit Name*** | ***Class*** | ***Rationale*** |
| --- | --- | --- |
|  | *(A,B,C)* |  |
|  |  |  |

**Level of Concern According to FDA:**

| ***System/Item/Unit Name*** | ***Class*** | ***Rationale*** |
| --- | --- | --- |
|  | *(Minor, Moderate, Major)* |  |
|  |  |  |

# Approvals

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name** | **Signature** | **Date** |
| **Software Development Manager** |  |  |  |
| **CEO** |  |  |  |

# Document Change Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version umber** | **Date** | **Author(s)** | **Brief Description of Change** |
| <<###>> | <<###>> | <<###>> | <<###-###>> |