PSES San Diego Chapter meeting – April 11, 2017

PSES
Product Safety Engineering Society
SAN DIEGO CHAPTER

CSA Group

Software, Risk Management, Usability, is Medical Device safety as we know it a thing of the past?

Naysahn Saeed
CSA Group

Goals for the session:

common understanding of the terms, concepts, and requirements

open discussion on the challenges ahead, as well as the benefits

Framework for our discussion

- Valuable tools for the development of new high tech devices
- Valuable tools for the development of combination devices
- Safe yesterday didn't become "unsafe" today.

5

Old process flow

Measurement

↓

Compare to Std. Req.

↓

Pass/Fail Decision

6

Panic

"Compliance is checked by inspection of the RISK MANAGEMENT FILE."

7

Panic?

"Compliance is checked by inspection of the RISK MANAGEMENT FILE."

8

Risk

9

RM in the 3rd Edition

Clause 4.2 : "A risk management process complying with ISO 14971 shall be performed."

Risk – used 631 times in IEC 60601-1
Risk Management – used 230 times in IEC 60601-1
Hazard –used 337 times in IEC 60601-1

10

RM in the 3rd Edition

"The RISK MANAGEMENT PROCESS should identify not only those HAZARDS addressed by this standard, but all HAZARDS, their associated RISKS and RISK CONTROL measures"

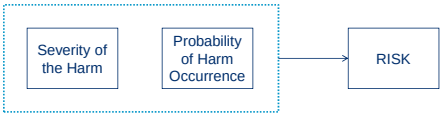
"Compliance with the clauses of this standard that contains specific, verifiable requirements is presumed to reduce the associated RISK(S) to an acceptable level"

11

Risk Management Refresher

Risk – Combination of the probability of occurrence of harm and the severity of that harm

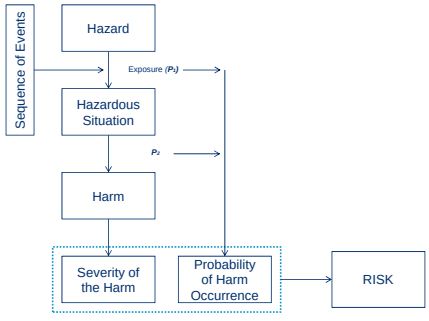
(Probability of Harm) x (Severity of Harm) = (Risk)



Source: ISO 14971

12

Risk Assessment



Source: ISO 14971

13

Risk Evaluation

14

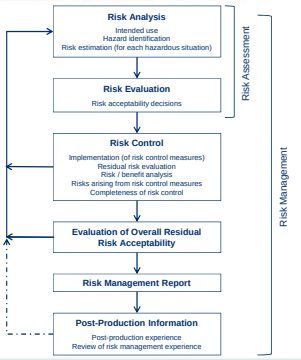
What is acceptable risk?

"**Where this standard or any collateral or particular standard specify verifiable requirements addressing particular RISKS, and these requirements are complied with, the RESIDUAL RISKS addressed by these requirements shall be presumed to be acceptable unless there is OBJECTIVE EVIDENCE to the contrary**"

15

Risk Management Overview

A process that continues and evolves throughout the product lifecycle:



16

Essential Performance

ESSENTIAL PERFORMANCE = performance necessary to achieve freedom from unacceptable RISK

NOTE: ESSENTIAL PERFORMANCE is most easily understood by considering whether its absence or degradation would result in an unacceptable RISK.

Ed 3.1: performance *of a clinical function, other than that related to BASIC SAFETY, where loss or degradation beyond the limits specified by the MANUFACTURER results in an* unacceptable RISK.

17

The World Has Changed (?)

The world has changed …

… but not as much as we might think

18

Safety

- Purpose and intention is still safety.
- Safety = Freedom from unacceptable risk

19

In Other Words …

ESSENTIAL PERFORMANCE = performance necessary to achieve freedom from unacceptable RISK.

ESSENTIAL PERFORMANCE = performance necessary to achieve SAFETY

SAFETY = freedom from unacceptable RISK

20

Safety for a Changing World

Basic Safety

Essential Performance

21

Safety

BASIC SAFETY – Baseline for safety for all devices

ESSENTIAL PERFORMANCE – additional basic safety specific to YOUR device

BASIC SAFETY Failure – your equipment doing something it shouldn't

ESSENTIAL PERFORMANCE Failure – your equipment failing to do something it should

22

Usability

Medical practice is increasingly using MEDICAL ELECTRICAL EQUIPMENT for observation and treatment of PATIENTS. USE ERRORS caused by inadequate MEDICAL ELECTRICAL EQUIPMENT USABILITY have become an increasing cause for concern. Much of ME EQUIPMENT developed without applying a USABILITY ENGINEERING PROCESS are non-intuitive, difficult to learn and to use. As healthcare evolves, less skilled OPERATORS including PATIENTS themselves are now using MEDICAL ELECTRICAL EQUIPMENT while the MEDICAL ELECTRICAL EQUIPMENT itself is becoming more complicated. In simpler times, the OPERATOR of the MEDICAL ELECTRICAL EQUIPMENT might be able to cope with an ambiguous, difficult-to-use OPERATOR-EQUIPMENT INTERFACE. The design of usable MEDICAL ELECTRICAL EQUIPMENT is a challenging endeavour. The design of the OPERATOR-EQUIPMENT INTERFACE to achieve adequate (safe) USABILITY requires a very different skill set than that of the technical implementation of that interface.

The USABILITY ENGINEERING PROCESS is intended to achieve reasonable USABILITY, which in turn is intended to minimise USE ERRORS and to minimise use-associated RISKS. Some, but not all, forms of incorrect use are amenable to be controlled by the MANUFACTURER.

23

Usability

24

Usability

Scope:

This International Standard specifies a PROCESS for a MANUFACTURER to analyse, specify, design, VERIFY and VALIDATE USABILITY, as it relates to BASIC SAFETY and ESSENTIAL PERFORMANCE of MEDICAL ELECTRICAL EQUIPMENT, hereafter referred to as ME EQUIPMENT.

This USABILITY ENGINEERING PROCESS assesses and mitigates RISKS caused by USABILITY problems associated with CORRECT USE and USE ERRORS, i.e., NORMAL USE. It can be used to identify but does not assess or mitigate RISKS associated with ABNORMAL USE.

25

Usability

ABNORMAL USE

intentional act or intentional omission of an act by the RESPONSIBLE ORGANIZATION or USER of a MEDICAL DEVICE as a result of conduct that is beyond any further reasonable means of RISK CONTROL by the MANUFACTURER

USE ERROR

act or omission of an act that results in a different MEDICAL DEVICE response than intended by the MANUFACTURER or expected by the USER

This International Standard uses the concept of USE ERROR. The term was chosen over the more commonly used terms of "user error" or "human error" because not all errors associated with the use of a MEDICAL DEVICE are the result of oversight or carelessness on the part of the USER of the MEDICAL DEVICE. Much more commonly, USE ERRORS are the direct result of poor USER INTERFACE design. Some USER INTERFACE designs contribute to USE ERROR because they employ non-intuitive or counter-intuitive displays or controls. The consequences of such design flaws often only become apparent when the USER is using the MEDICAL DEVICE in an emergency or stressful situation, is fatigued, or uses the MEDICAL DEVICE only rarely.

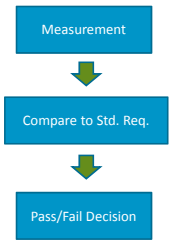
26

Usability

Bringing design for use to the forefront

27

Old process flow



28

Usability and Risk Management

29

Software

Prevalence

Reliance

30

Software

Purpose

This standard defines the life cycle requirements for MEDICAL DEVICE SOFTWARE. The set of PROCESSES, ACTIVITIES, and TASKS described in this standard establishes a common framework for MEDICAL DEVICE SOFTWARE life cycle PROCESSES.

Compliance

Compliance with this standard is defined as implementing all of the PROCESSES, ACTIVITIES, and TASKS identified in this standard in accordance with the software safety class.

Compliance is determined by inspection of all documentation required by this standard including the RISK MANAGEMENT FILE, and assessment of the PROCESSES, ACTIVITIES and TASKS required for the software…

31

PROGRAMMABLE ELECTRICAL MEDICAL SYSTEMS (PEMS)

The requirements … shall apply to PEMS unless:

– none of the PROGRAMMABLE ELECTRONIC SUBSYSTEM (PESS) provides functionality necessary for BASIC SAFETY or ESSENTIAL PERFORMANCE; or

– the application of RISK MANAGEMENT as described in 4.2 demonstrates that the failure of any PESS does not lead to an unacceptable RISK.

The requirements in 14.13 are applicable to any PEMS intended to be incorporated into an IT NETWORK whether or not the requirements in 14.2 to 14.12 apply.

32

PEMS

14.11 * PEMS VALIDATION

A PEMS VALIDATION plan shall include the validation of BASIC SAFETY and ESSENTIALPERFORMANCE.

Methods used for PEMS VALIDATION shall be documented.

The PEMS VALIDATION shall be performed according to the PEMS VALIDATION plan. The results of PEMS VALIDATION activities shall be documented.

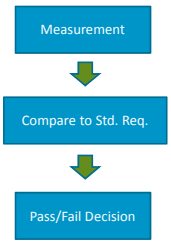
The person having the overall responsibility for the PEMS VALIDATION shall be independent of the design team. The MANUFACTURER shall document the rationale for the level of independence.

No member of a design team shall be responsible for the PEMS VALIDATION of their own design.

All professional relationships of the members of the PEMS VALIDATION team with members of the design team shall be documented in the RISK MANAGEMENT FILE.

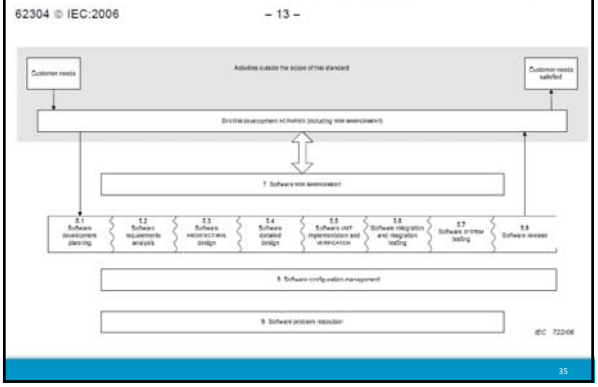
33

Old process flow



34

Overview of software development PROCESSES and ACTIVITIES



35

Home Healthcare

INTRODUCTION

Medical practice is increasingly using MEDICAL ELECTRICAL EQUIPMENT and MEDICAL ELECTRICAL SYSTEMS for monitoring, treatment or diagnosis of PATIENTS in the HOME HEALTHCARE ENVIRONMENT (see 3.1). The safety of MEDICAL ELECTRICAL EQUIPMENT in this uncontrolled environment with regard to the electrical installation and its related safety and protection means is a cause for concern.

The potential lack of training of the LAY OPERATOR and possibly of those supervising the use of the MEDICAL ELECTRICAL EQUIPMENT or MEDICAL ELECTRICAL SYSTEM and their level of education need to be addressed in the development of the ACCOMPANYING DOCUMENTS and in the relevant marking on the equipment itself so that this material can be understood. This collateral standard gives special guidance on how this should be addressed in the instructions for use.

36

Changing Environment

Smart watches

Sleep tracking

Is regulation and standardization keeping up?

Cross functional involvement

37

Thank You for Your Time

Questions?

38

CSA Group