UNIVERSITÀ
DEGLI STUDI DI TRIESTE

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

ISTITUTO DI RICOVERO E CURA
A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste

BURLO

units

Dispositivi medici software una sfida globale: una nuova era dei dispositivi medici

La sicurezza informatica dei dispositivi medici

Antonio Bartolozzi

antonio.bartolozzi@bartolozzi.it

Trieste 25/11/2019

Health Software

2.17 ISO 29321:2008/TS
health software product
software product for use in the health sector for health related purposes but excluding software that is:

– necessary for the proper application of a medical device;
– an accessory to a medical device;
– a medical device in its own right.

NOTE 1 This definition is intended for this Technical Specification only.

3.6 EN 82304:2016
HEALTH SOFTWARE
software intended to be used specifically for maintaining or improving health of individual persons, or the delivery of care

Draft IEC 62304 Ed. 2: Health software - Software life cycle processes

3.11
HEALTH SOFTWARE
SOFTWARE SYSTEM intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a MEDICAL DEVICE

Note 1 to entry: HEALTH SOFTWARE fully includes what is considered software as a MEDICAL DEVICE.

[SOURCE: ISO 81001-1:—, 3.22, modified — In the definition, the term "software" has been replaced by "SOFTWARE SYSTEM".]

DRAFT EN 62304 Ed. 2

3.9
HAZARD
potential source of HARM
Note 1 to entry: Potential sources of HARM include breach of SECURITY and reduction of effectiveness.

Under preparation. Stage at the time of this CDV: ISO/DIS 81001-1:2019.

3.10
HAZARDOUS SITUATION
circumstance in which people, property or the environment is/are exposed to one or more HAZARD(S)

ISO 81001-1:—, 3.17]

NEW

ISO 14971:2019 Benefit

3.2

benefit

positive impact or desirable outcome of the use of a medical device (3.10) on the health of an individual, or a positive impact on patient management or public health

Note 1 to entry: *Benefits* can include positive impact on clinical outcome, the patient's quality of life, outcomes related to diagnosis, positive impact from diagnostic devices on clinical outcomes, or positive impact on public health.

3.3

harm

injury or damage to the health of people, or damage to property or the environment

[SOURCE: ISO/IEC Guide 63:2019, 3.1]

IEC 80001-2010

2.8 harm

physical injury or damage to the health of people, or damage to property or the environment, or reduction in effectiveness, or breach of data and systems security

Software intended to specifically be used for delivery of care

DRAFT EN 62304

3.11
HEALTH SOFTWARE
SOFTWARE SYSTEM intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a MEDICAL DEVICE

Note 1 to entry: HEALTH SOFTWARE fully includes what is considered software as a MEDICAL DEVICE.

[SOURCE: ISO 81001-1:XXXX, 3.22, modified — In the definition, the term "software" has been replaced by "SOFTWARE SYSTEM".]

(53) 'clinical benefit' means the positive impact of a device on the health of an individual, expressed in terms of a meaningful, measurable, patient-relevant clinical outcome(s), including outcome(s) related to diagnosis, or a positive impact on patient management or public health;

European Commission
Medical Devices Regulation
EU MDR

MPI, ADT
healthcare booking system
C.U.P.?

Prevention of malfunctioning, as of an organ or structure of the body.

Class I ?

~~Software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes is classified as class IIa~~

ISO 14971:2019

— It is explained that the *process* described in ISO 14971 can be used for managing *risks* associated with *medical devices*, including those related to data and systems security.

GDPR & MDR

Directive 95/46/EC is repealed with effect from 25 May 2018

Article 110

Data protection

1. Member States shall apply Directive 95/46/EC to the processing of personal data carried out in the Member States pursuant to this Regulation.

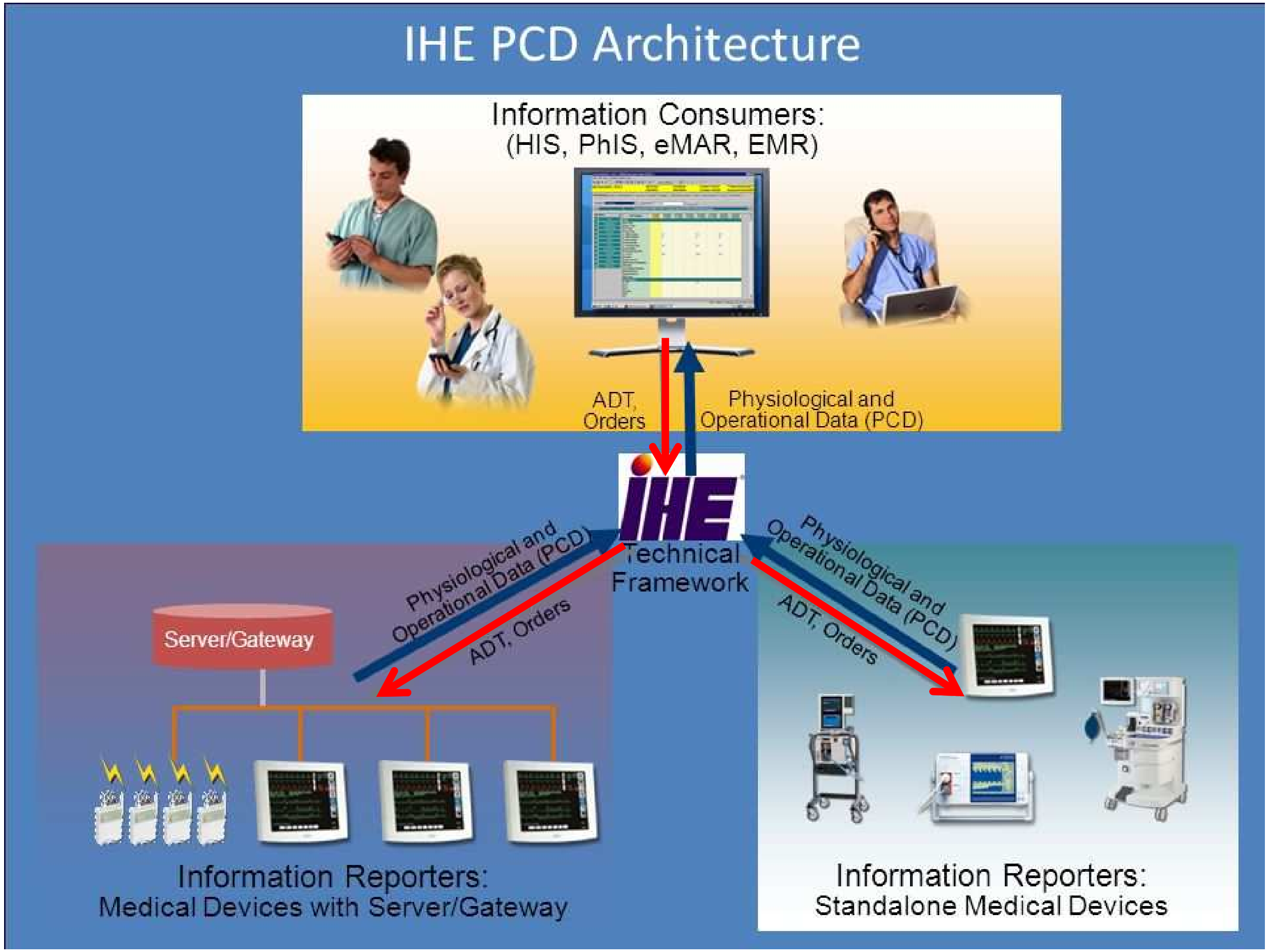
2. Regulation (EC) No 45/2001 shall apply to the processing of personal data carried out by the Commission pursuant to this Regulation.

EUDPR - Regulation 2018/1725

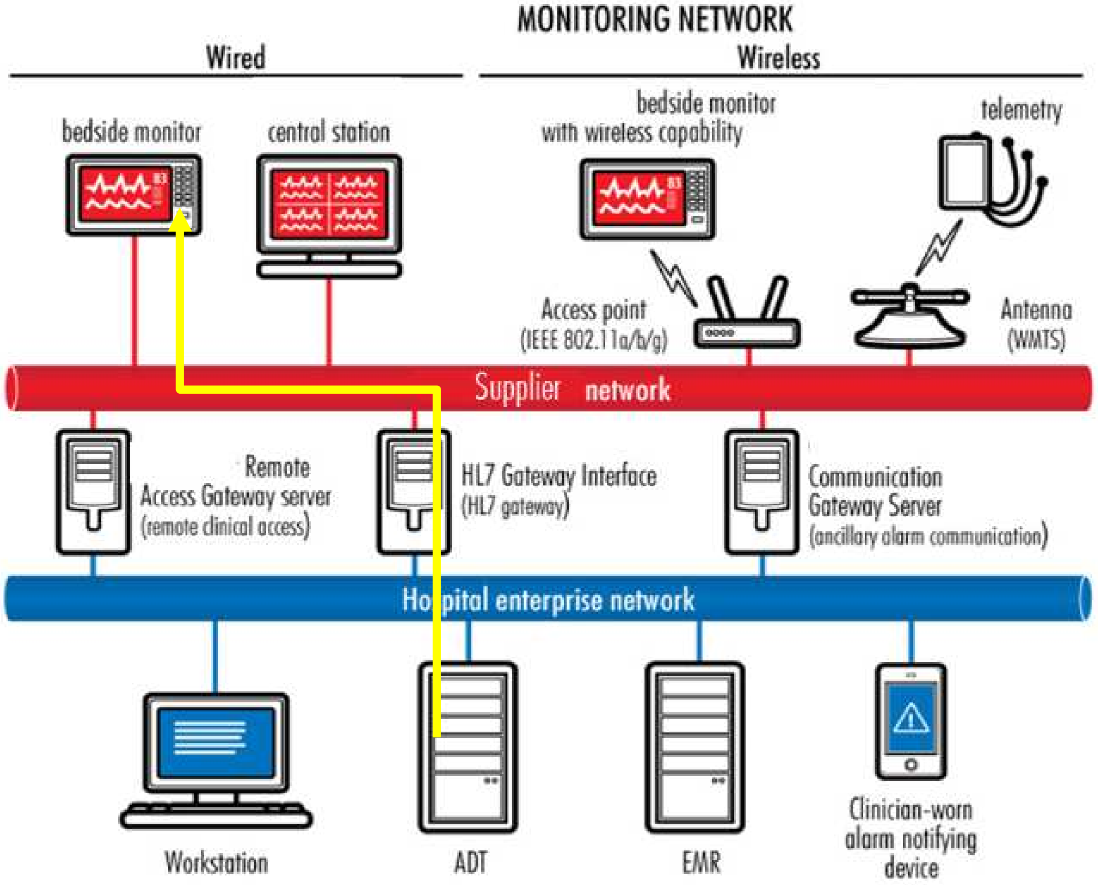
GDPR (EU 679/2016)

1.This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions and bodies and rules relating to the free movement of personal data between them or to other recipients established in the Union

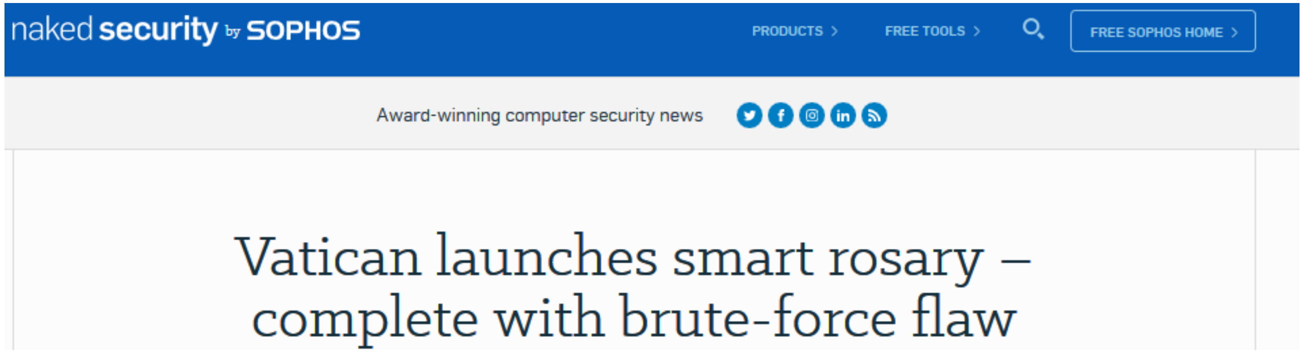
IHE PCD


IHE PCD Architecture
Information Consumers:
(HIS, PhIS, eMAR, EMR)
ADT, Orders
Physiological and Operational Data (PCD)
IHE
Technical Framework
Physiological and Operational Data (PCD)
ADT, Orders
Server/Gateway
Physiological and Operational Data (PCD)
ADT, Orders
Information Reporters:
Medical Devices with Server/Gateway
Information Reporters:
Standalone Medical Devices

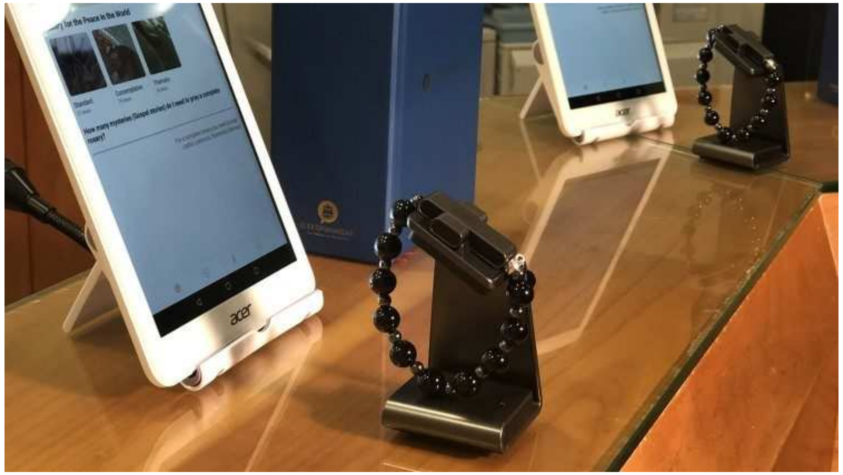
Vulnerability


MONITORING NETWORK
Wired
Wireless
bedside monitor
central station
bedside monitor with wireless capability
telemetry
Access point (IEEE 802.11a/b/g)
Antenna (WMTS)
Supplier network
Remote Access Gateway server (remote clinical access)
HL7 Gateway Interface (HL7 gateway)
Communication Gateway Server (ancillary alarm communication)
Hospital enterprise network
Workstation
ADT
EMR
Clinician-worn alarm notifying device

Smart Rosario – Not so smart



Vatican launches smart rosary – complete with brute-force flaw



Click to Pray

When a user resets their account using Click to Pray's app, it uses an application programming interface (API) to make the request to the server, which then sends the PIN to the user's email. The server also returns the PIN in its response to the API request, meaning that someone accessing the API directly could get the user's PIN without having access to their email.

Tomcat Realm

The standard Tomcat Realm component allows unlimited authorization attempts, opening the door to brute force attacks from a spoofed IP address. The LockOut Realm prevents this by placing a limit on the number of log in attempts within a given time period before a user is locked out of the system.

Draft EN 62304 – Risk Management

The MANUFACTURER of HEALTH SOFTWARE shall establish and maintain the following:

a) A PROCESS for managing RISKS, primarily to the patient, but also to the operator, other persons, property, and the environment. This PROCESS shall provide methods for identifying HAZARDS, performing RISK ESTIMATION and RISK EVALUATION, controlling identified RISKS, and monitoring the effectiveness of the RISK CONTROL measures, taking the INTENDED USE of the HEALTH SOFTWARE into account.

b) As applicable, a PROCESS for managing RISKS associated with SECURITY. This PROCESS shall provide methods for identifying vulnerabilities, estimating and evaluating the associated threats, controlling these threats, and monitoring the effectiveness of the RISK CONTROL (SECURITY) measures, taking the INTENDED USE of the HEALTH SOFTWARE into account.

NOTE 2 Examples of SECURITY RISK considerations and RISK CONTROL measures can be found in the ISO 27000 family of Information Security Management System (ISMS) standards (see Table C.1), ISO 27799 [19], IEC 62443 (all parts) [5], and AAMI TIR 57:2016 [30].

State of the art - ISO/IEC Guide 63:2019

3.18

state of the art

developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience.

Note 1 to entry: The state of the art embodies what is currently and generally accepted as good practice in technology and medicine. **The state of the art does not necessarily imply the most technologically advanced solution**. The state of the art described here is sometimes referred to as the “**generally acknowledged state of the art**”.

[SOURCE: ISO/IEC Guide 2:2004, 1.4, modified — Note 1 to entry has been added.]

ISO/EN 14971:2012 Annex D - Risk concepts applied to medical devices

“State of the art” is used here to mean what is currently and generally accepted as good practice. **Various methods can be used to determine "state of the art"** for a particular medical device.

Examples are:

- **standards used for the same or similar devices;**
- **best practices as used in other devices of the same or similar type;**
- results of accepted scientific research.

ISO 24971:2013 - Developing the policy for determining the criteria for risk acceptability

When developing or maintaining the **policy** (for determining the criteria for risk acceptability) the following should be taken into consideration:

— The **applicable regulatory requirements in the regions where the medical device is to be marketed**.
— The **relevant International Standards for the particular medical device or an intended use of the medical device that can help identify principles for setting the criteria for risk acceptability** (see 2.2).
— **Information on the state of the art can be obtained from review of the literature and other information on similar medical devices the manufacturer has marketed, as well as those from competing companies**.
— The validated and comprehensive concerns from the main stakeholders. Some potential sources of information on the patient and clinician perspective can include news media, social media, patient forums, as well as input from internal departments with expert knowledge of stakeholder concerns such as the clinical department.

Priority in the state of art

Directive 2001/95/CE

In the absence of specific European standards /common specifications, the safety and security of products should be assessed taking into account in particular national standards transposing any other relevant European or international standards, European Commission recommendations or national standards, international standards, codes of good practice/best practices, results of accepted scientific research and other state of the art documents.

You can apply (in the following order of priority) :

- **harmonized standards (CEN) or European common specifications;**
- national standards transposing any other relevant European or international standards
- **European Commission recommendations**
- applicable regulatory requirements in the European country where the medical device is to be marketed;
- **relevant International Standards (IEC, ISO, AAMI, IEEE) for the particular medical device or an intended use of the medical device;**
- best practices (FDA, Health Canada, Australia's Therapeutic Goods Administration, …) as used in other devices of the same or similar type;
- results of accepted scientific research.

GENERAL SAFETY AND PERFORMANCE REQUIREMENTS n. 1

1. Devices shall achieve the performance intended by their manufacturer and shall be designed and manufactured in such a way that, during normal conditions of use, they are suitable for their intended purpose. They shall be safe and effective and shall not compromise the clinical condition or the safety of patients, or the safety and health of users or, where applicable, other persons, provided that any risks which may be associated with their use constitute acceptable risks when weighed against the benefits to the patient and are compatible with a high level of protection of health and safety, taking into account the generally acknowledged **state of the art.**

GENERAL SAFETY AND PERFORMANCE REQUIREMENTS n. 4

4. **Risk control measures** adopted by manufacturers for the design and manufacture of the devices shall conform to safety principles, taking account of the generally acknowledged **state of the art**. To reduce risks, Manufacturers shall manage risks so that the residual risk associated with each hazard as well as the overall residual risk is judged acceptable. In selecting the most appropriate solutions, manufacturers shall, in the following order of priority:

(a) eliminate or reduce risks as far as possible through safe design and manufacture;

(b) where appropriate, take adequate protection measures, including alarms if necessary, in relation to risks that cannot be eliminated; and

(c) provide information for safety (warnings/precautions/contra-indications) and, where appropriate, training to users.

Manufacturers shall inform users of any residual risks.

REQUIREMENTS REGARDING DESIGN AND MANUFACTURE

Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves

17.2. For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance ***with the state of the art*** *taking into account the principles of development life cycle,* ***risk management****,* ***including information security****, verification and validation.*

Electronic programmable systems – Essential principles of safety and performance

17.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.

EN 62304
EN 14971
EN 82304

ISO 80001-1
ISO 80001-2-1
ISO 80001-2-2
ISO 80001-2-4

ISO/IEC 27701
ISO/IEC 27001
AAMI TIR57, Principles for medical device security—Risk management

There is no «*the state of the art*» authorization ➔ Only **Harmonizated Standards have the presumption of conformity** (Sorry!)

You can still use relevant International Standards but without the presumption of conformity : please prepare a justification that explains the need for this standards (it is quite easy !)

Electronic programmable systems – Essential principles of safety and performance

17.2. For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance ***with the state of the art*** *taking into account the principles of development life cycle,* ***risk management****,* ***including information security****, verification and validation.*

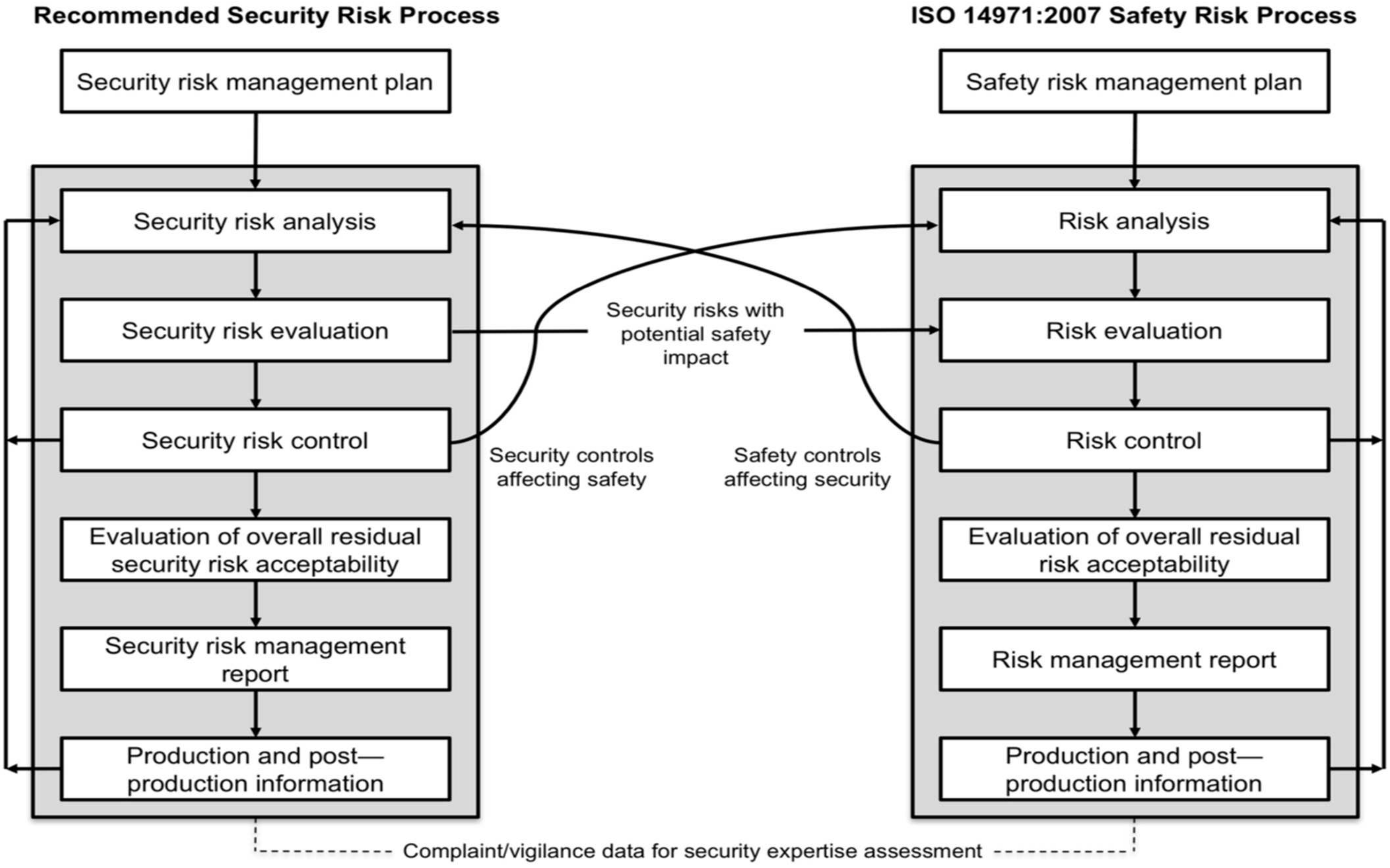
EN 60601-1
EN 62304
EN 14971
EN 82304

ISO 80001-1
ISO 80001-2-1
ISO 80001-2-2
ISO 80001-2-4
AAMI TIR57/Ed. 1, Principles for medical device security—Risk management

You can apply (in the following order of priority) :

- **harmonized standards (CEN) or European Commission recommendations/common specifications;**
- applicable regulatory requirements in the European country where the medical device is to be marketed;
- **relevant International Standards (IEC, ISO, AAMI, IEEE) for the particular medical device or an intended use of the medical device;**
- best practices (FDA, Health Canada, Australia’s Therapeutic Goods Administration, …) as used in other devices of the same or similar type;
- results of accepted scientific research.

AAMI TIR 57

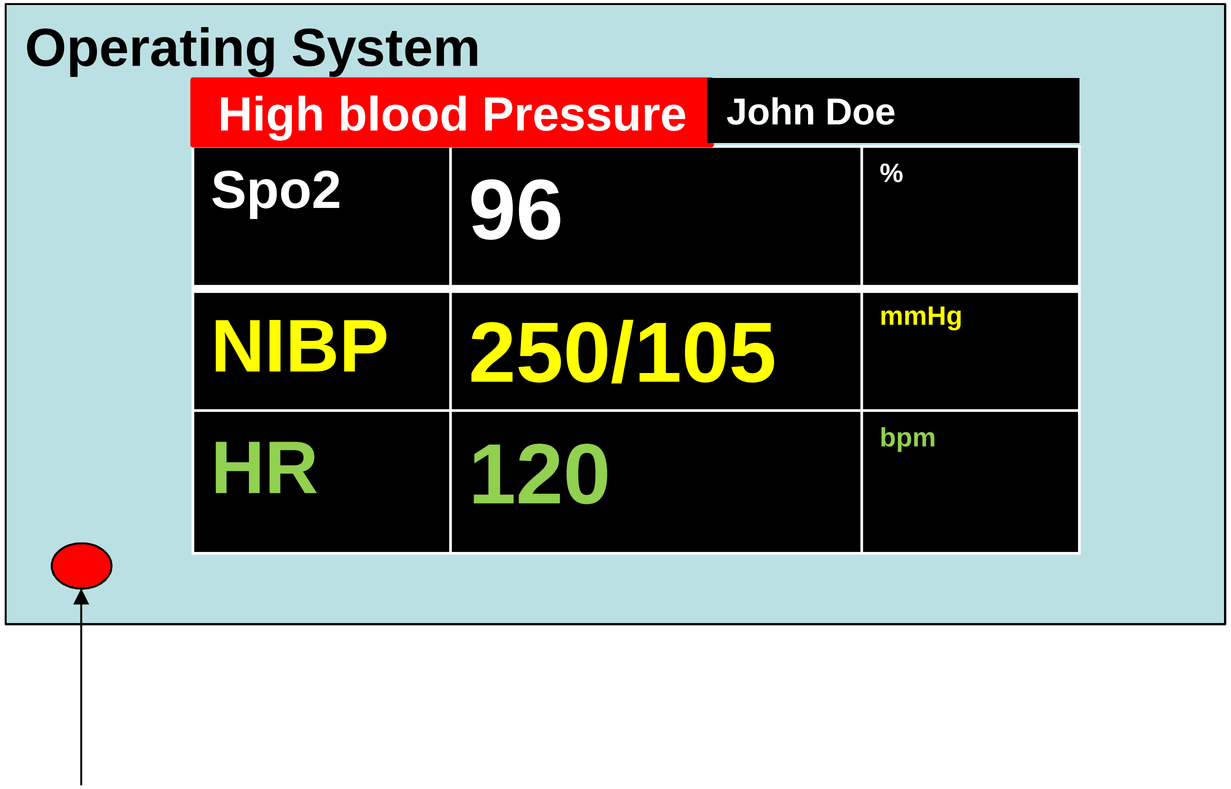


Recommended Security Risk Process
ISO 14971:2007 Safety Risk Process
Security risk management plan
Security risk analysis
Security risk evaluation
Security risk control
Evaluation of overall residual security risk acceptability
Security risk management report
Production and post—production information
Safety risk management plan
Risk analysis
Risk evaluation
Risk control
Evaluation of overall residual risk acceptability
Risk management report
Production and post—production information
Security risks with potential safety impact
Security controls affecting safety
Safety controls affecting security
Complaint/vigilance data for security expertise assessment

AAMI TIR 57

Because threats change over time and new vulnerabilities in operating systems, middleware and components are discovered on regular basis, security risks are frequently identified after a device is released to the market.

Operating system vulnerability

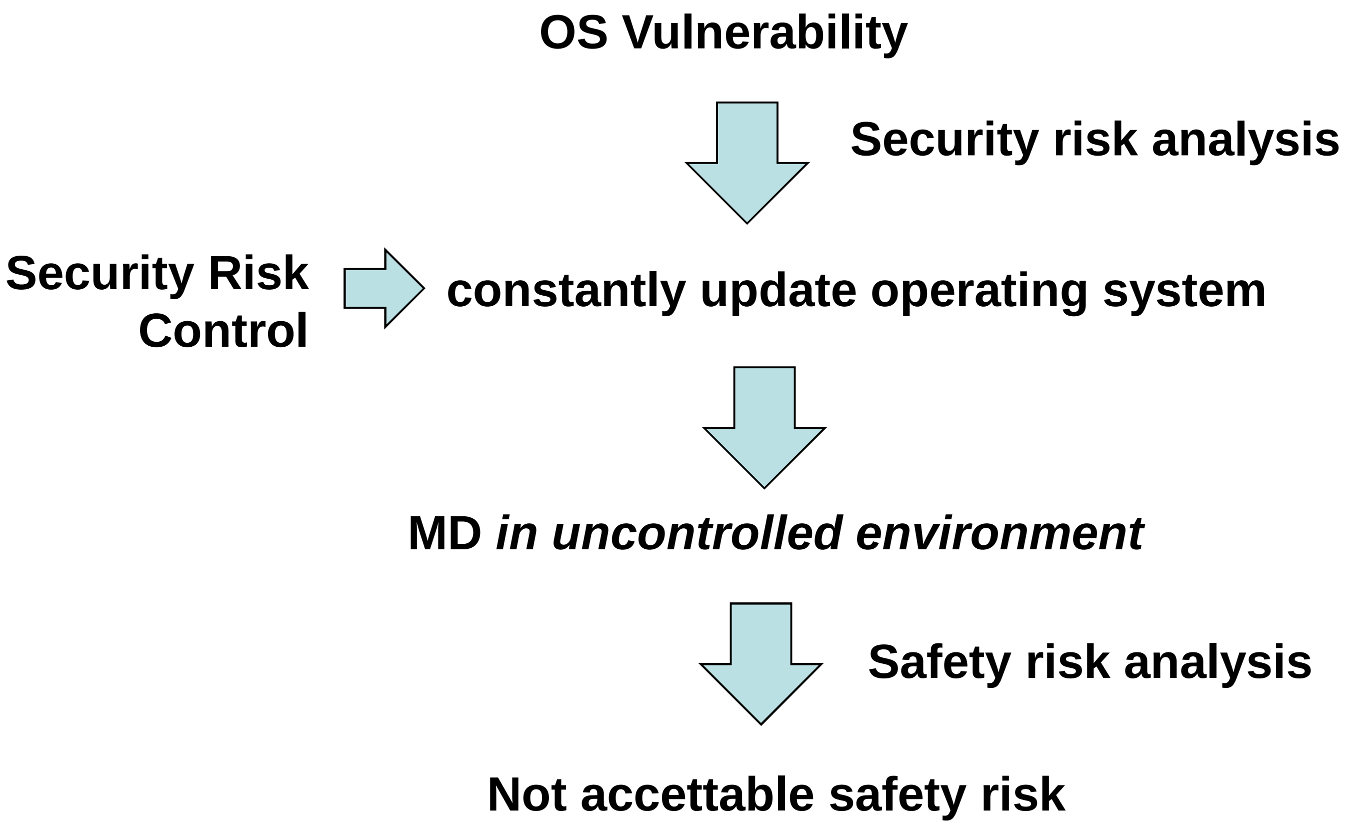


Operating System

High blood Pressure		John Doe
Spo2	96	%
NIBP	250/105	mmHg
HR	120	bpm

Vulnerability

AAMI TIR57 Risk Analysis – Security → Safety



OS Vulnerability

Security risk analysis

Security Risk Control

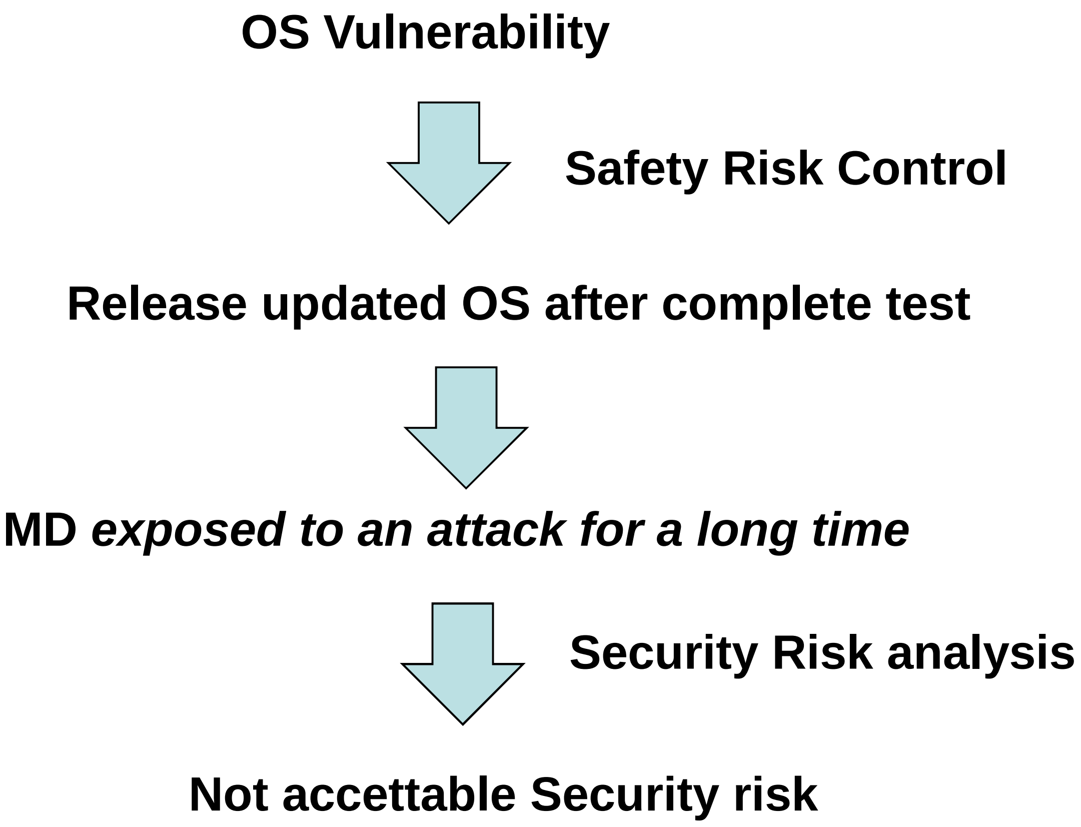
constantly update operating system

MD *in uncontrolled environment*

Safety risk analysis

Not accettable safety risk

AAMI TIR57 Risk Analysis – Safety ➔ Security



OS Vulnerability

Safety Risk Control

Release updated OS after complete test

MD *exposed to an attack for a long time*

Security Risk analysis

Not accettable Security risk

New Design - GPI’s Medical device

- NEOCARE - Neonatal Intensive Care Unit (NICU)
- ASTER TOTAL CARE – Telemedicine (Veneto region)

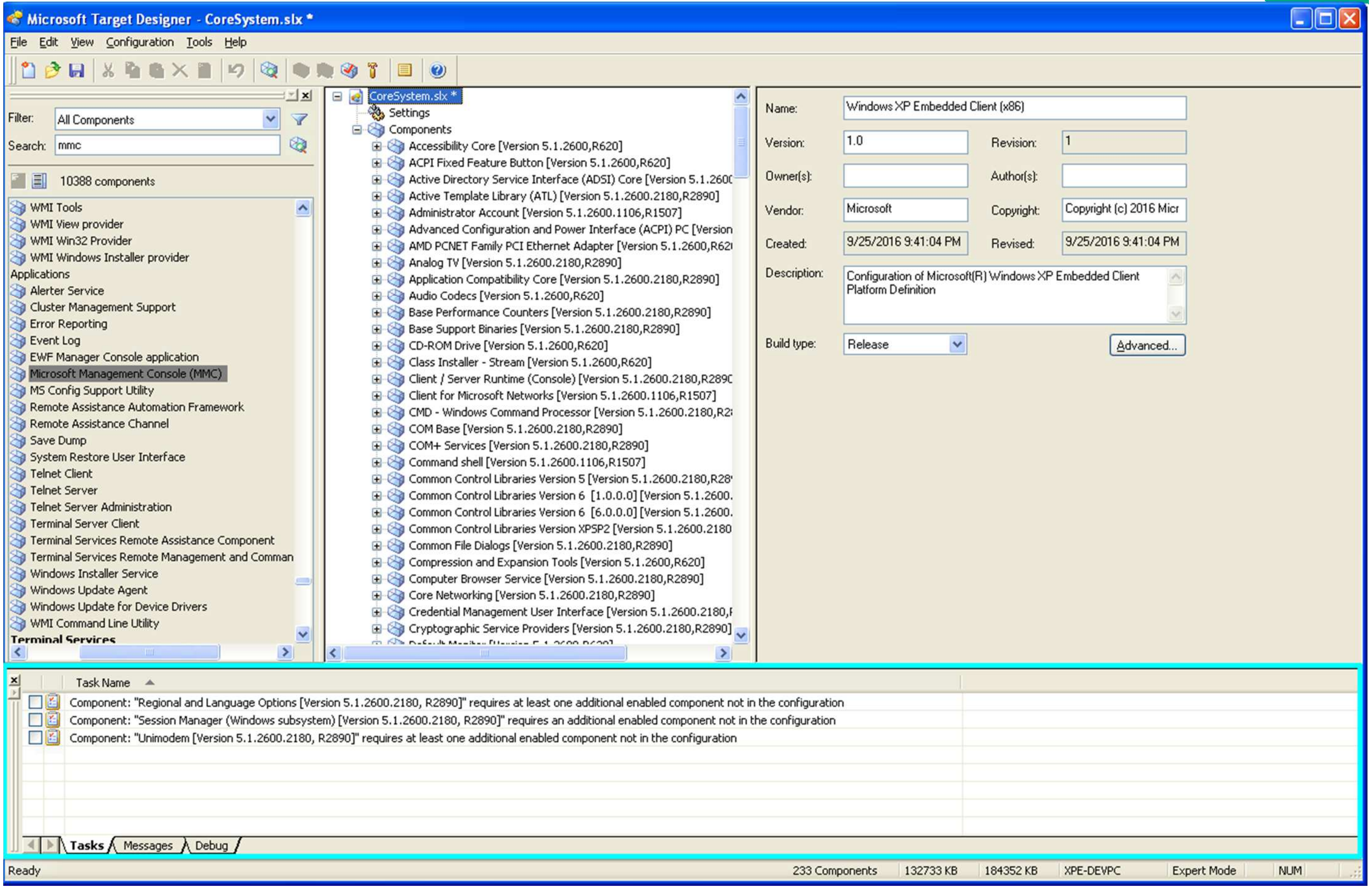
Change design

- **Minimize Operating system**
- **New OP security barriers**

LEGO-like Operating system

- ***Strong firewall whitelist* based**
- **Advanced *Operating System Process Manager***

Example - Windows XP Embedded


Microsoft Target Designer - CoreSystem.slx *
File Edit View Configuration Tools Help
Tasks
Messages
Debug
Advanced...

Filter: All Components

Search: mmc

10388 components

- WMI Tools
- WMI View provider
- WMI Win32 Provider
- WMI Windows Installer provider

Applications

- Alerter Service
- Cluster Management Support
- Error Reporting
- Event Log
- EWF Manager Console application
- Microsoft Management Console (MMC)
- MS Config Support Utility
- Remote Assistance Automation Framework
- Remote Assistance Channel
- Save Dump
- System Restore User Interface
- Telnet Client
- Telnet Server
- Telnet Server Administration
- Terminal Server Client
- Terminal Services Remote Assistance Component
- Terminal Services Remote Management and Comman
- Windows Installer Service
- Windows Update Agent
- Windows Update for Device Drivers
- WMI Command Line Utility

Terminal Services

CoreSystem.slx *

- Settings
- Components
  - Accessibility Core [Version 5.1.2600,R620]
  - ACPI Fixed Feature Button [Version 5.1.2600,R620]
  - Active Directory Service Interface (ADSI) Core [Version 5.1.2600
  - Active Template Library (ATL) [Version 5.1.2600.2180,R2890]
  - Administrator Account [Version 5.1.2600.1106,R1507]
  - Advanced Configuration and Power Interface (ACPI) PC [Version
  - AMD PCNET Family PCI Ethernet Adapter [Version 5.1.2600,R62
  - Analog TV [Version 5.1.2600.2180,R2890]
  - Application Compatibility Core [Version 5.1.2600.2180,R2890]
  - Audio Codecs [Version 5.1.2600,R620]
  - Base Performance Counters [Version 5.1.2600.2180,R2890]
  - Base Support Binaries [Version 5.1.2600.2180,R2890]
  - CD-ROM Drive [Version 5.1.2600,R620]
  - Class Installer - Stream [Version 5.1.2600,R620]
  - Client / Server Runtime (Console) [Version 5.1.2600.2180,R289
  - Client for Microsoft Networks [Version 5.1.2600.1106,R1507]
  - CMD - Windows Command Processor [Version 5.1.2600.2180,R2
  - COM Base [Version 5.1.2600.2180,R2890]
  - COM+ Services [Version 5.1.2600.2180,R2890]
  - Command shell [Version 5.1.2600.1106,R1507]
  - Common Control Libraries Version 5 [Version 5.1.2600.2180,R28
  - Common Control Libraries Version 6 [1.0.0.0] [Version 5.1.2600.
  - Common Control Libraries Version 6 [6.0.0.0] [Version 5.1.2600.
  - Common Control Libraries Version XPSP2 [Version 5.1.2600.2180
  - Common File Dialogs [Version 5.1.2600.2180,R2890]
  - Compression and Expansion Tools [Version 5.1.2600,R620]
  - Computer Browser Service [Version 5.1.2600.2180,R2890]
  - Core Networking [Version 5.1.2600.2180,R2890]
  - Credential Management User Interface [Version 5.1.2600.2180,R
  - Cryptographic Service Providers [Version 5.1.2600.2180,R2890]

Name: Windows XP Embedded Client (x86)

Version: 1.0 Revision: 1

Owner(s): Author(s):

Vendor: Microsoft Copyright: Copyright (c) 2016 Micr

Created: 9/25/2016 9:41:04 PM Revised: 9/25/2016 9:41:04 PM

Description: Configuration of Microsoft(R) Windows XP Embedded Client Platform Definition

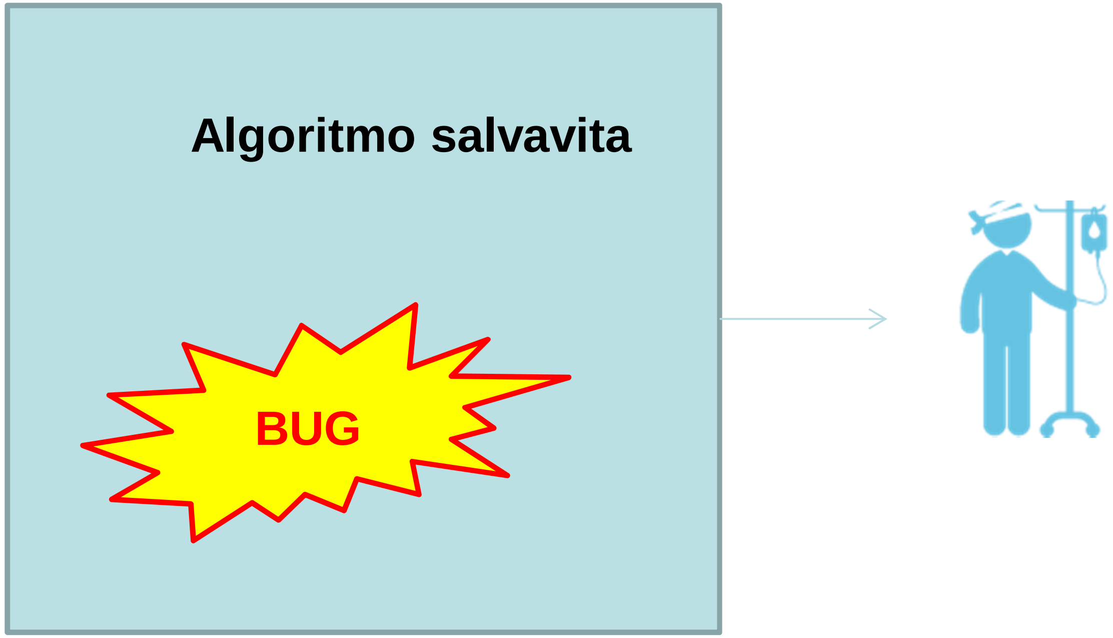
Build type: Release

Task Name

- ☐ Component: "Regional and Language Options [Version 5.1.2600.2180, R2890]" requires at least one additional enabled component not in the configuration
- ☐ Component: "Session Manager (Windows subsystem) [Version 5.1.2600.2180, R2890]" requires an additional enabled component not in the configuration
- ☐ Component: "Unimodem [Version 5.1.2600.2180, R2890]" requires at least one additional enabled component not in the configuration

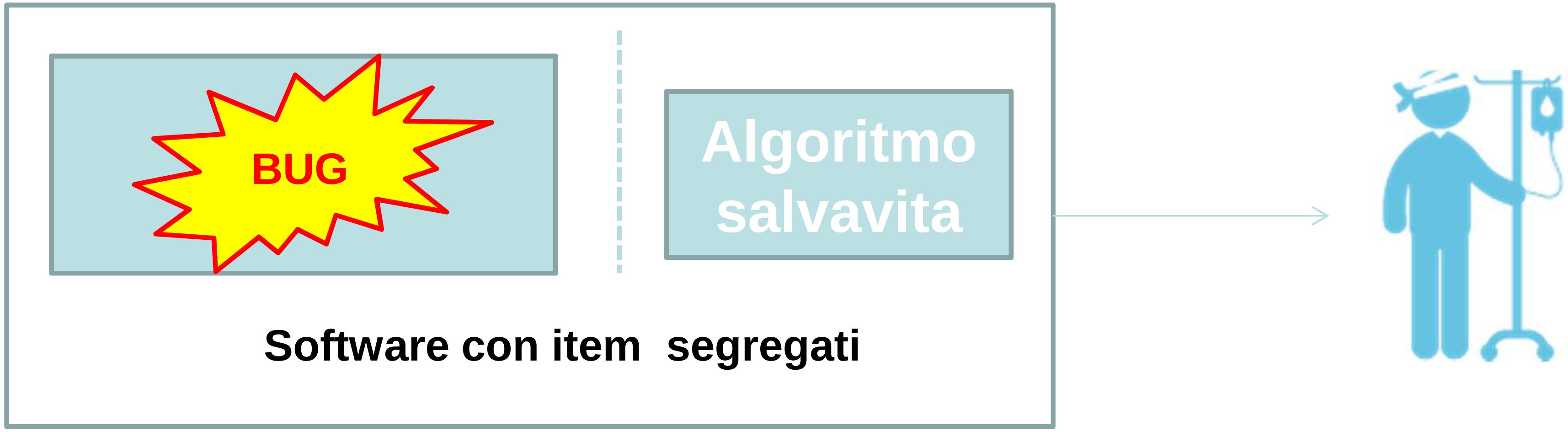
Ready | 233 Components | 132733 KB | 184352 KB | XPE-DEVPC | Expert Mode | NUM

Architetture monolitiche



Nelle architetture monolitiche una qualsiasi parte del programma o dei sistemi usati per farlo girare (sistema operativo, application server) sono in grado di compromettere la capacità di adempiere allo scopo previsto del dispositivo medico

Architetture segregate



Nelle architetture segregate le parti principali del programma sono protette dai bug del resto dei componenti dell'architettura. Un bug presente in una qualsiasi parte del sistema non può compromettere totalmente la capacità di adempiere allo scopo previsto del dispositivo medico.

Albert Sabin (1)

- La sconfitta definitiva della poliomielite si deve al vaccino di Albert Sabin (1906-1993).
- Un ragazzino nato cieco da un occhio che ha salvato il mondo.
  Il cacciatore di sogni. Lo scienziato che salvò il mondo
  Sara Rattaro (Mondadori)
- L’introduzione ritardata del vaccino Sabin in Italia si calcola abbia causato almeno 10.000 casi di poliomielite con più di 1.000 decessi ed oltre 8000 paralisi

Sabin

«Tanti insistevano che brevettassi il vaccino, ma non ho voluto. È il mio regalo a tutti i bambini del mondo»