Use of risk analysis techniques ISO 14971 - Suggested text for 24971

There is a great deal of confusion between engineering techniques used for dealing with failures and risk analysis/management.

To understand the differences, it's important to understand where risk management comes from.

In the beginning of the 1900s, with the event of the industrial revolution, more complex systems were being developed and manufactured (mass manufacturers). One of the problems identified in products in general was that they could fail, in particular due to design or manufacturing problems. This gave rise to the concept of reliability (reliability existed before because it's a product characteristic, but the codification of a reliability engineering field begun in the early 1900s).

NOTE FROM MARCELO _ THE FOLLOWING figure illustrate this, but it comes from a copyrighted document, so I'm using it for information only. From Saleh, J.H., Marais, K. (2006). "Highlights from the early (and pre-) history of reliability engineering", Reliability Engineering & System Safety, vol. 91, no. 2, pp. 249-256.

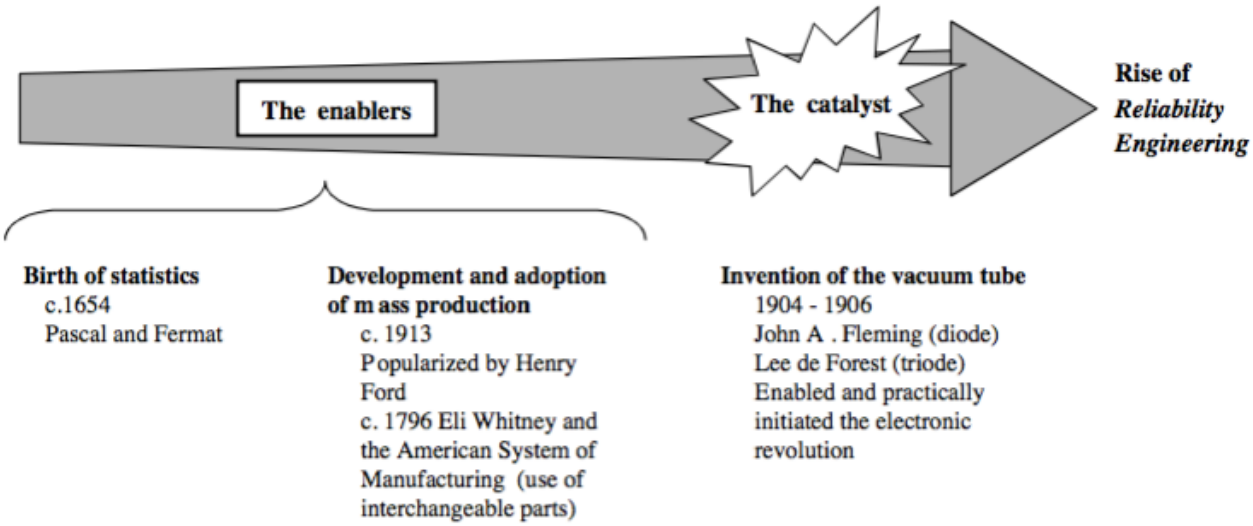


Fig. 1. Enablers and the catalyst of reliability engineering: statistics, mass production, and the vacuum tube.

Reliability is defined as (IEC 192-01-24):

reliability, <of an item>

ability to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration can be expressed in units appropriate to the item concerned, e.g. calendar time, operating cycles, distance run, etc., and the units should always be clearly stated.

Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.
Note 3 to entry: Reliability can be quantified using measures defined in Section 192-05, Reliability related concepts: measures.

Thus, reliability is a characteristic of any product, related to the ability to perform as required, without failure, for a given time interval, under given conditions. It's related to availability.

One of the differences between reliability and other characteristics of a product is that reliability cannot be tested into a product (a reliability test can only demonstrated which reliability the product was designed and manufactured to achieve).

Reliability is usually described in means of the probability of success or the frequency of failures.

Reliability engineering deal with the design and manufacturing of products in a way that failures are reduced and thus a defined success is achieved. Several different techniques were created to evaluate failures rates and thus be used for failure analysis as part of the reliability engineering process.

For example, FMEA was developed in the 1950s by the US Millitary (MIL-P-1629:1949) for equipment and system analysis.

FTA was developed by the Bell Telephone Laboratories in 1962 use by the US Air Force in the reliability evaluation of the Minuteman I Intercontinental Ballistic Missile (ICBM) Launch Control System.

What is important to understand is that these techniques are focused in failure of product/system and the effect on the product/system (meaning, when the product/system loses its ability to perform, related to the definition of reliability).

They are also not focused on safety (which is other, separate characteristic of product/systems). For example, a product/system can be reliable and unsafe, or it can loose its ability to perform in an unsafe way.

As products grew more complex and dangerous, another development which took place was the codification of system safety, which focused not only on reliability but also on safety.

NOTE FROM MARCELO _ THE FOLLOWING figure illustrate this, but it comes from a copyrighted document, so I'm using it for information only. From Saleh, J.H., Marais, K. (2006). "Highlights from the early (and pre-) history of reliability engineering", Reliability Engineering & System Safety, vol. 91, no. 2, pp. 249-256.

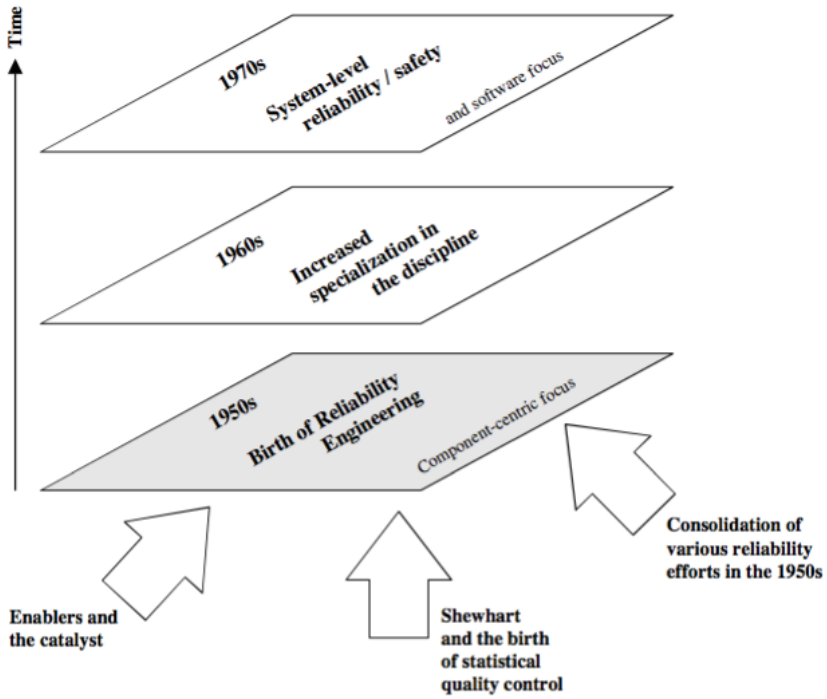


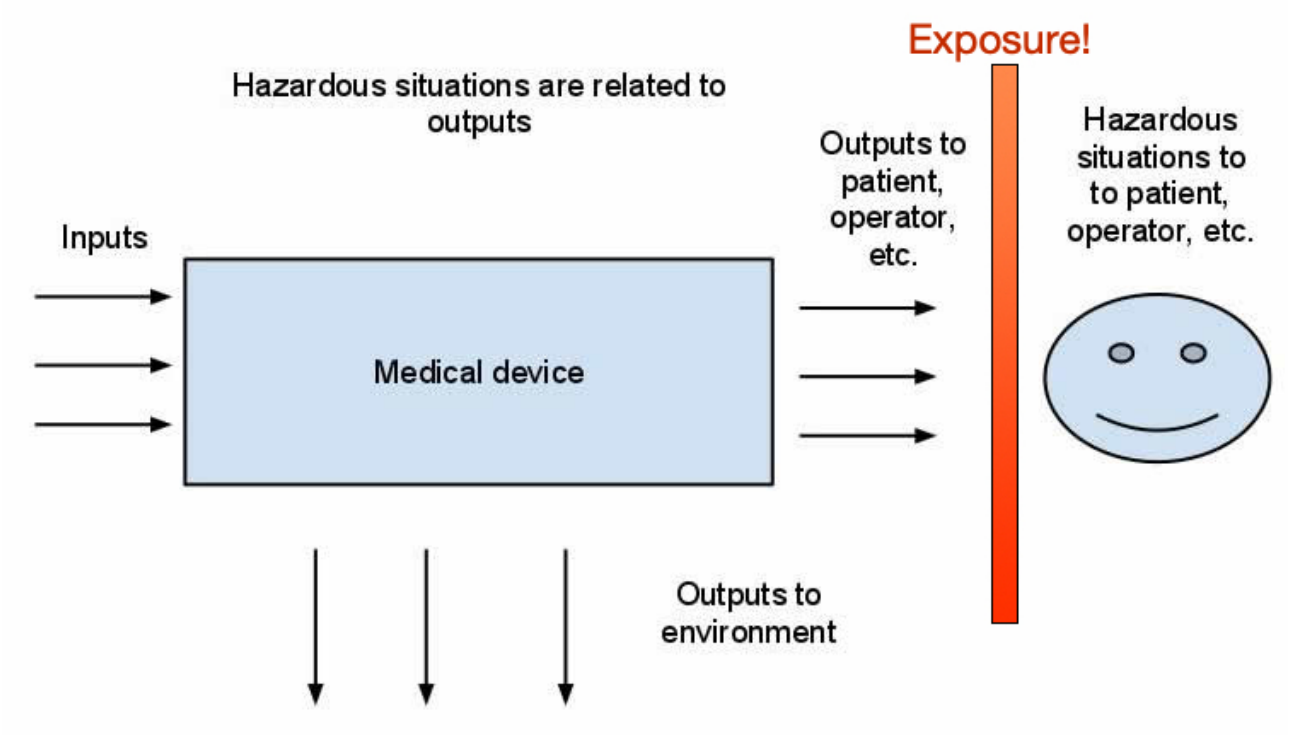
Fig. 3. Three decades and three phases in the development of reliability engineering.

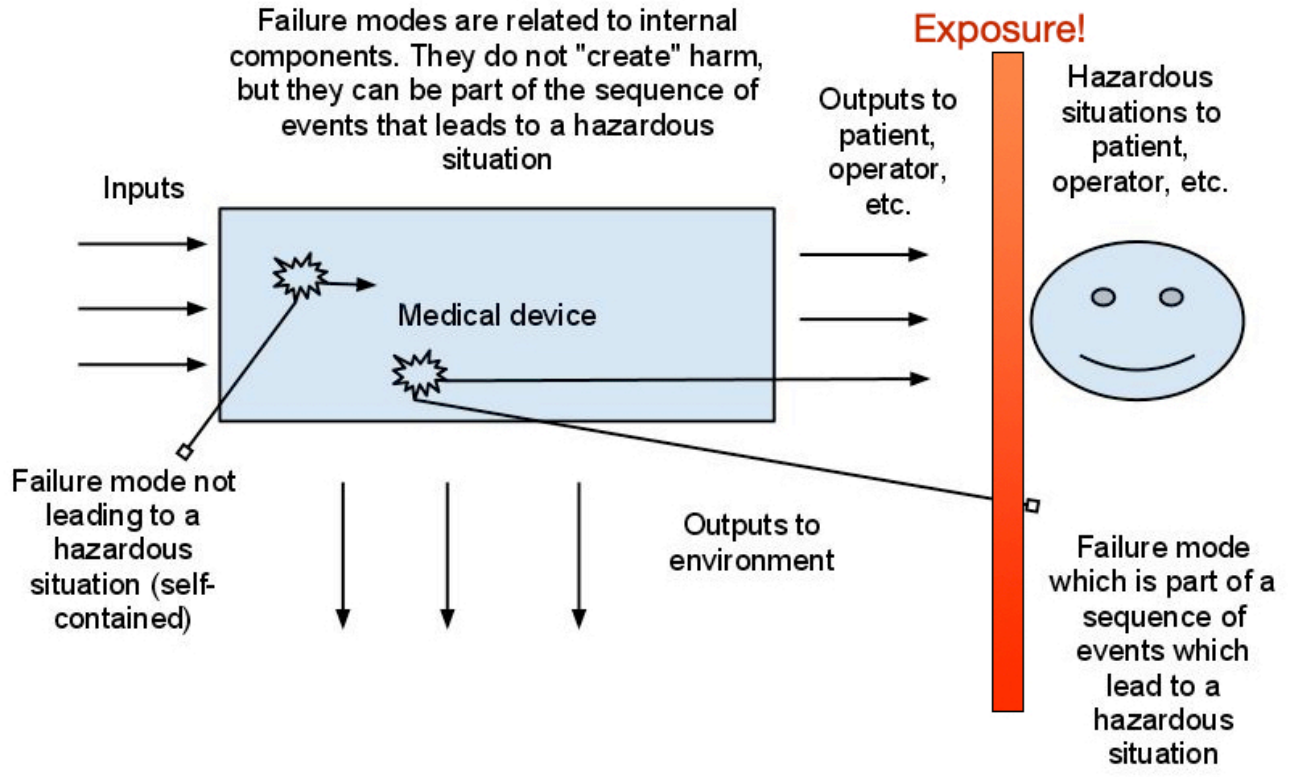
Failures modes are internal to a product/system, and can influence the reliability/availability of the system.

Some (not necessarily all) failure modes can be part of the sequence of events that lead to hazardous situations, for example, to the patient/user, However, the historical techniques for failure analysis focus on internal failures only, and their impact on the devices.

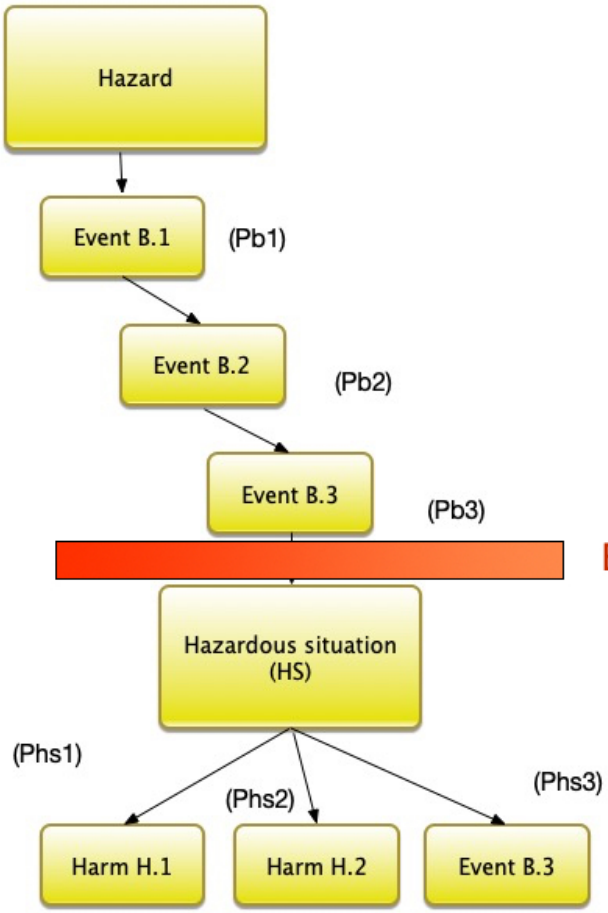
For a hazard situation to occur, and thus to harm to occur to a patient/user, there must be exposure (to the patient/user), and historical failure analysis techniques do not include this option as they deal only with "internal". Thus, for any technique used, some additional steps need to be included, depending on how far the technique goes.

NOTE FROM MARCELO _ THE FOLLOWING 3 figures were created by me, based on an old presentation by Oliver Christ



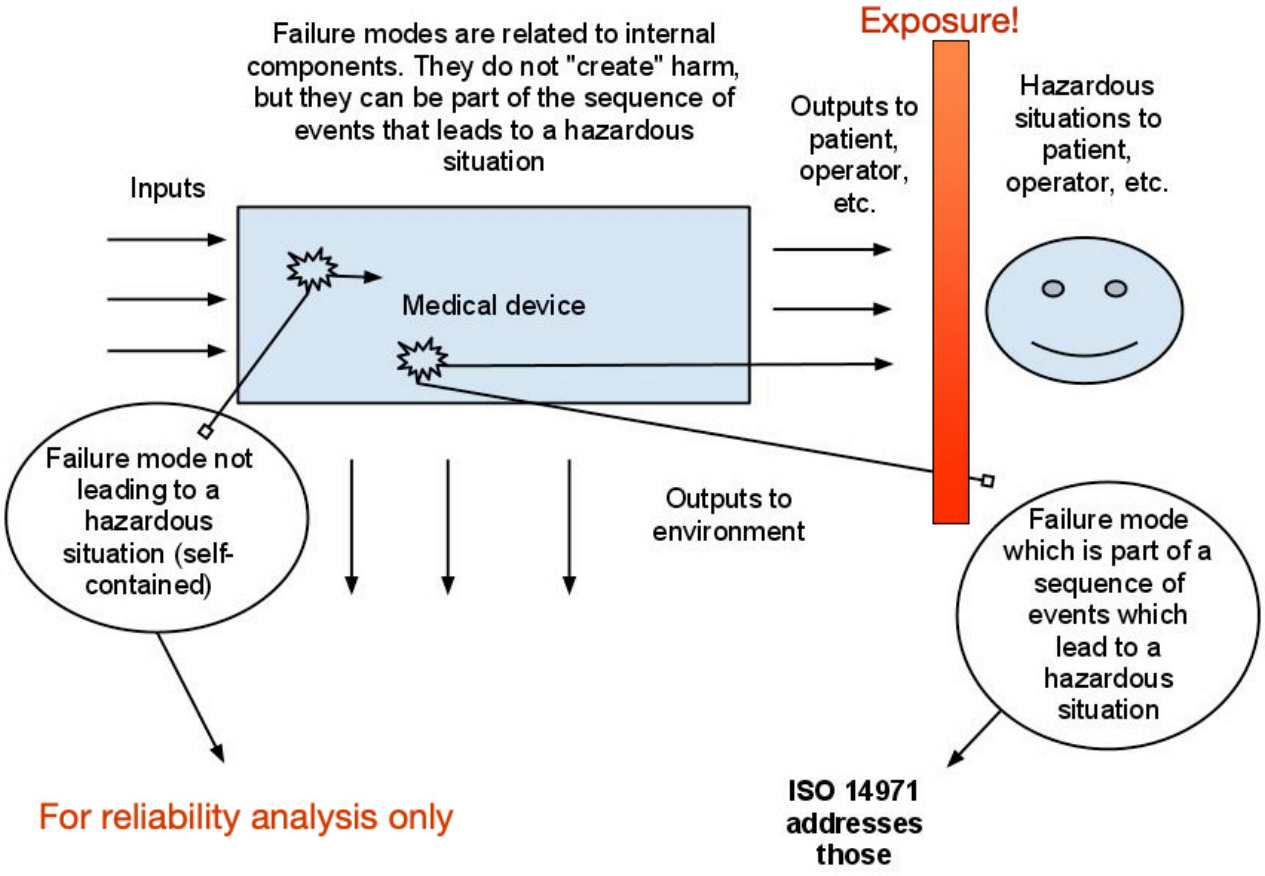


Hazard, hazardous situation and risk - probabilities (adapted from Medical Device Software Verification_ Validation and Compliance)

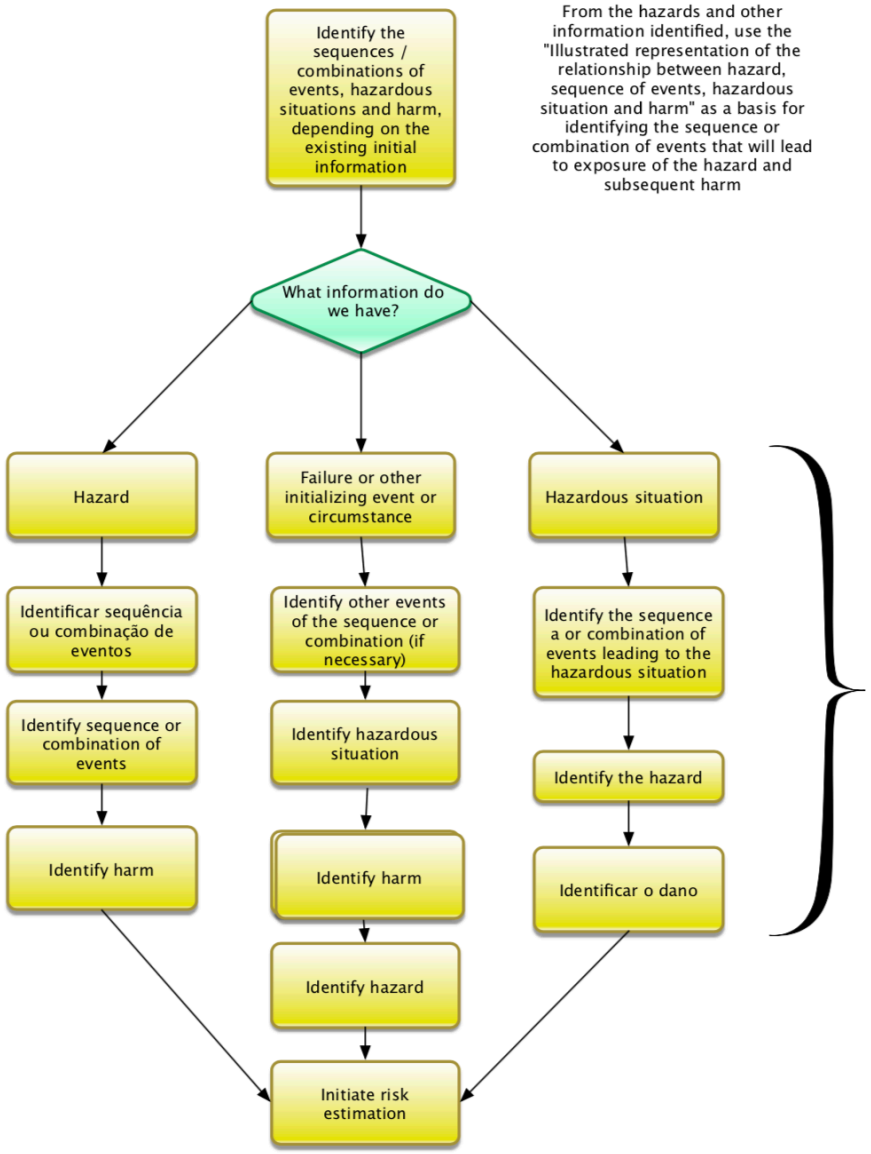


Exposure!

Failure analysis technique usually stop here, which is the boundary on which happens to the device)


Failure modes are related to internal components. They do not "create" harm, but they can be part of the sequence of events that leads to a hazardous situation
Exposure!
Inputs
Outputs to patient, operator, etc.
Hazardous situations to patient, operator, etc.
Medical device
Failure mode not leading to a hazardous situation (self-contained)
Outputs to environment
Failure mode which is part of a sequence of events which lead to a hazardous situation
For reliability analysis only
ISO 14971 addresses those

One general way to think about using any technique is to focus on which information we have and A general way to think about using techniques is: which information I've got, and which information is still lacking? See figure below



From the hazards and other information identified, use the "Illustrated representation of the relationship between hazard, sequence of events, hazardous situation and harm" as a basis for identifying the sequence or combination of events that will lead to exposure of the hazard and subsequent harm

Identify sources to get data

a) Published standards
b) Technical and scientific data
c) Field data of similar medical devices
already in use, including reports of published incidents
d) Usability tests with the participation of typical users
e) Clinical evidence
f) Results of appropriate investigations
g) Expert opinion
h) External quality assessment schemes

Identify techniques / analysis tools to identify the data. Depending on the information we, different techniques will be required to identify the missing information (for example, if we have the hazardous situation, a deductive technique such as FTA is required. If we have the initial hazard, a inductive technique such as FMEA is required

Check, throughout the use of analysis techniques / tools, all initializing events and circumstances in Table E.2