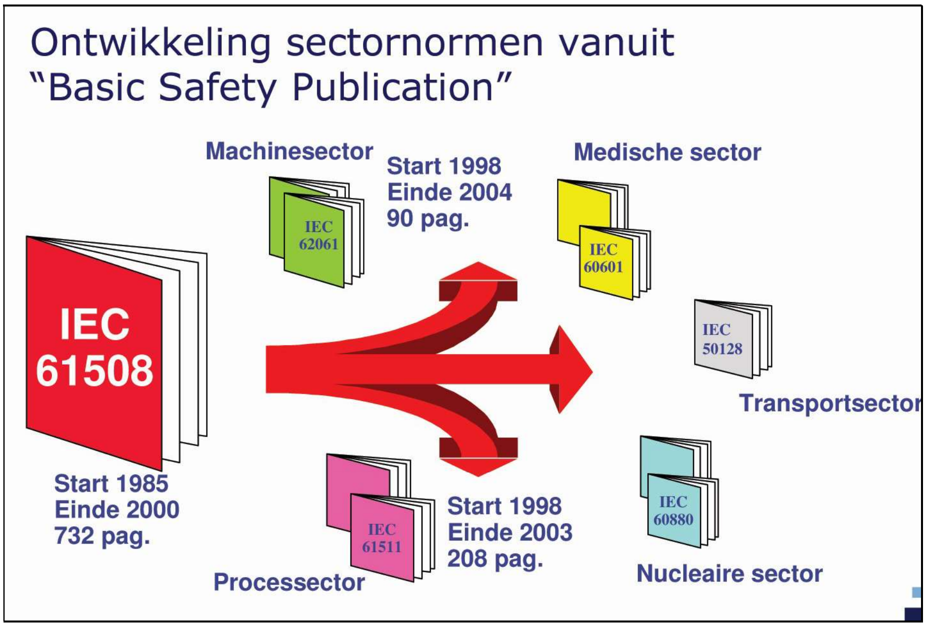
Title: Functional safety applied in instrumentation technology and process automation.

Introduction :

Every company experiences daily that there are risks in the execution of certain work or business processes that can lead to undesirable situations. This can cause all kinds of damage such as: accident damage to people and installation, environmental damage, economic damage and image damage. It is necessary to know the risks in advance and to take measures against these dangers.

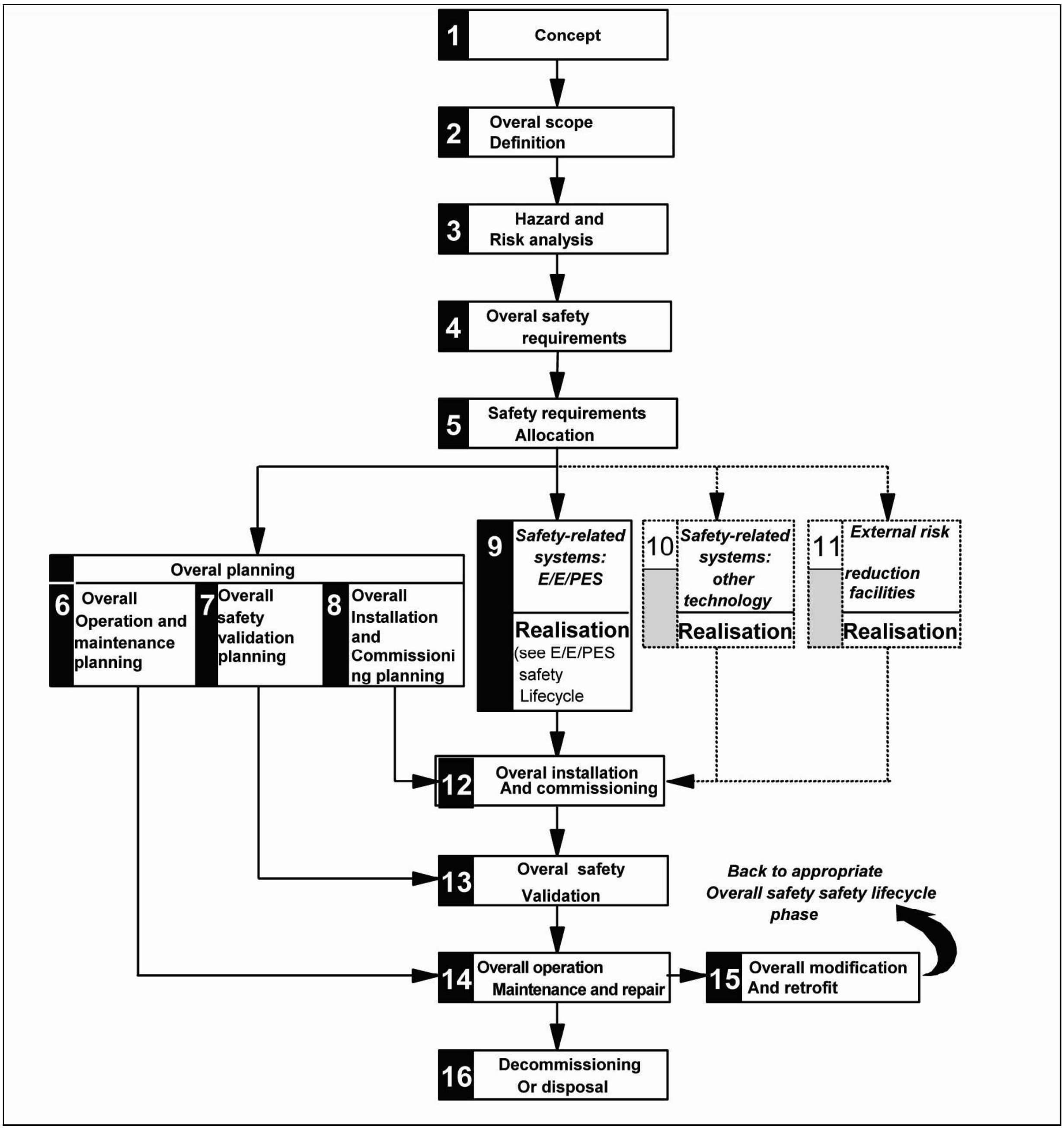
Various laws and guidelines have been developed to determine and guarantee the functional safety of installations. Since 1996, the ISA standard S84.01 has been used in the USA, whichApplication of Safety Instrumented Systems for the Process IndustriesIn Europe, IEC 61508 came into force in 2000 and describes:Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems and is very general and conceptual. Derived from this is the IEC61511 and came into force in 2003, it describes: Instrumented Systems for the process industry Sector. This describes the 'Safety Lifecycle' concept, the minimum requirements for hardware and software and indicates how the SIL level must be determined. There is (as yet) no legal obligation for this standard, but it does offer a structured methodology that is easy to audit. The methodology can be easily integrated into any internal 'safety management system'. Graphically, this IEC legislation can be represented as follows:



-Figure 1 Development of IEC safety standards.

Safety Lifecycle (SLC) and SIL:

The inventory and assessment of risks is done cyclically, i.e. it must be repeated after a period of time, taking into account experiences and new insights. Security measures must also be evaluated and possibly improved. The entire life cycle of the process therefore applies from design to demolition of the process installation. This can be shown as follows:

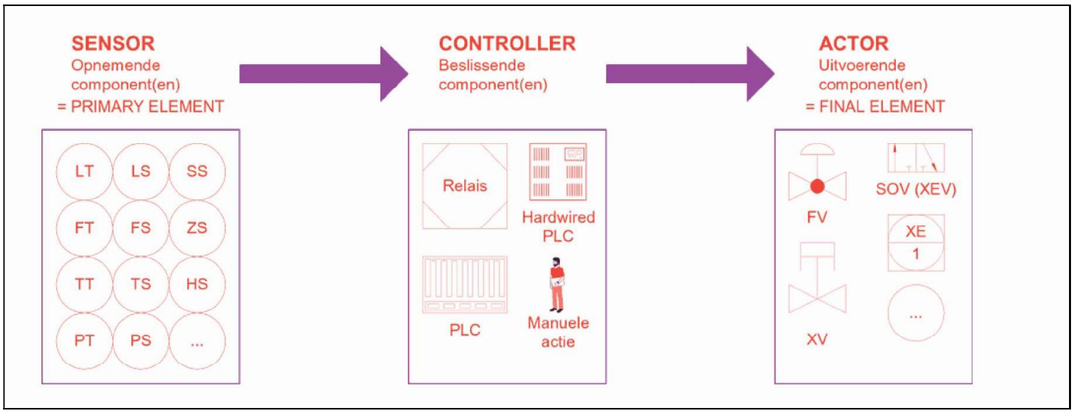

1 Concept
2 Overal scope Definition
3 Hazard and Risk analysis
4 Overal safety requirements
5 Safety requirements Allocation
Overal planning
6 Overall Operation and maintenance planning
7 Overall safety validation planning
8 Overall Installation and Commissioning planning
9 Safety-related systems: E/E/PES
Realisation (see E/E/PES safety Lifecycle
10 Safety-related systems: other technology
Realisation
11 External risk reduction facilities
Realisation
12 Overal installation And commissioning
13 Overal safety Validation
Back to appropriate Overall safety safety lifecycle phase
14 Overall operation Maintenance and repair
15 Overall modification And retrofit
16 Decommissioning Or disposal

-Figure 2 Safety Life cycle.

The SLC can thus be grouped as follows: step 1-5 = analytical measures; step 6-13 = application measures; step 14-16 = in-service measures.

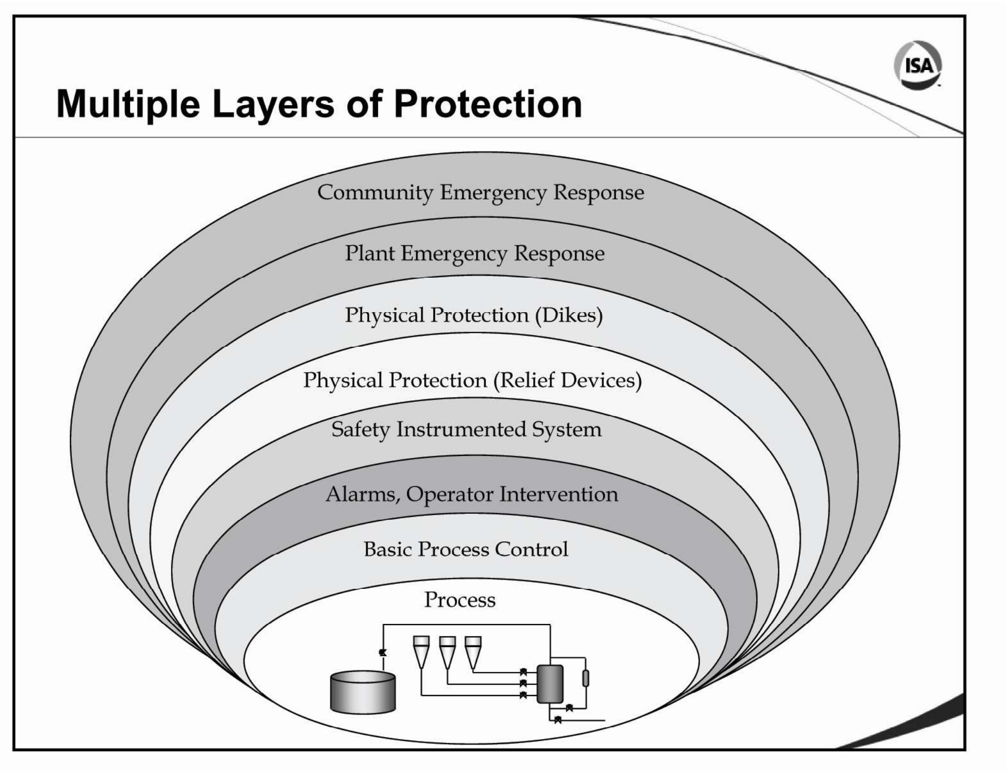
Risk inventory assessment is performed by means of a HAZOP study (Hazard and Operatibility Analysis). The probability that an event with damage occurs multiplied by the extent of the damage provides the level of risk. In IEC61508 this is called the SIL level (Safety Integrity Level). This SIL level requires a certain quality of the safety provision(s).

The SIL level of a process can be achieved by protecting critical functions in the process and thus reducing the risk; these functions are called SIFs (Safety Integrity Function). A process protection provision is called a SIS (Safety Integrity System). A SIS consists of several instrumental components. Each component can cause a complete trip of the SIS. A SIS could therefore protect several SIFs. A SIS therefore looks like this:



-Figure 3 A SIS

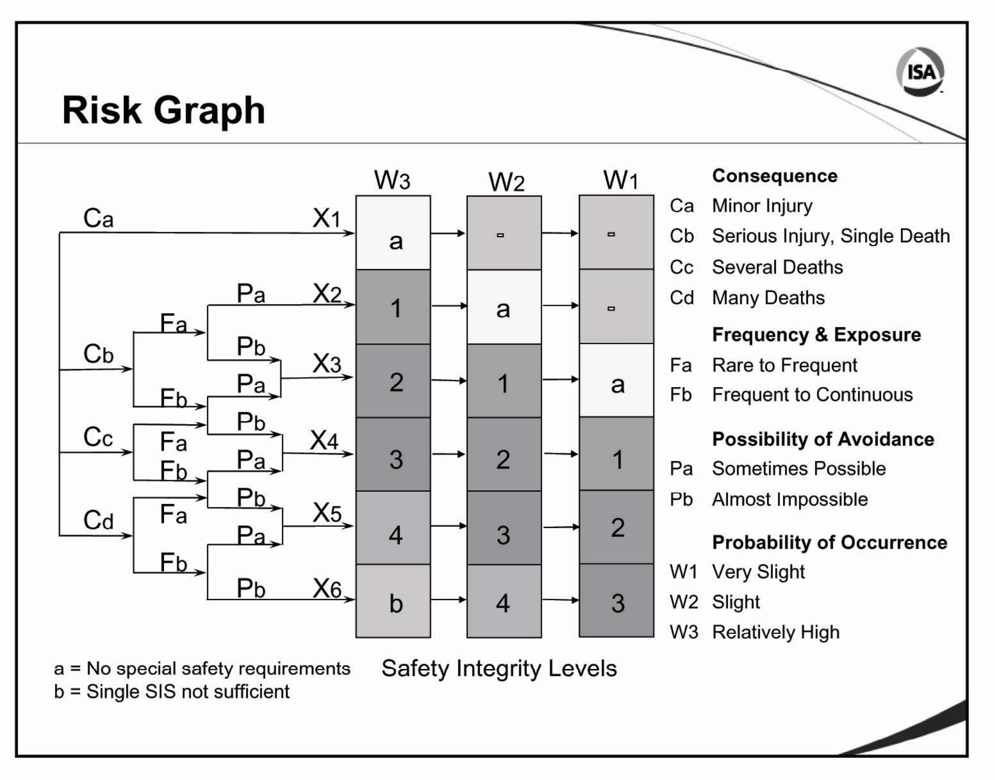
In the USA, process protection measures are divided into layers, the so-called LOPA system (Layers Of Protection). The SIS is part of this. The LOPA system looks like this:


Multiple Layers of Protection
ISA
Community Emergency Response
Plant Emergency Response
Physical Protection (Dikes)
Physical Protection (Relief Devices)
Safety Instrumented System
Alarms, Operator Intervention
Basic Process Control
Process

-Figure 4 LOPA system

Risk graph:

The SIL level therefore expresses how well a system must perform its safety function in order to achieve the required risk reduction. There are 4 levels: 1 = flexible / 4
= extremely high. The SIL level can be determined by means of a risk graph; this looks like this:



Risk Graph

	W3	W2	W1
X1	a	▫	▫
X2	1	a	▫
X3	2	1	a
X4	3	2	1
X5	4	3	2
X6	b	4	3

Safety Integrity Levels

a = No special safety requirements
b = Single SIS not sufficient

Consequence

Ca	Minor Injury
Cb	Serious Injury, Single Death
Cc	Several Deaths
Cd	Many Deaths

Frequency & Exposure

Fa	Rare to Frequent
Fb	Frequent to Continuous

Possibility of Avoidance

Pa	Sometimes Possible
Pb	Almost Impossible

Probability of Occurrence

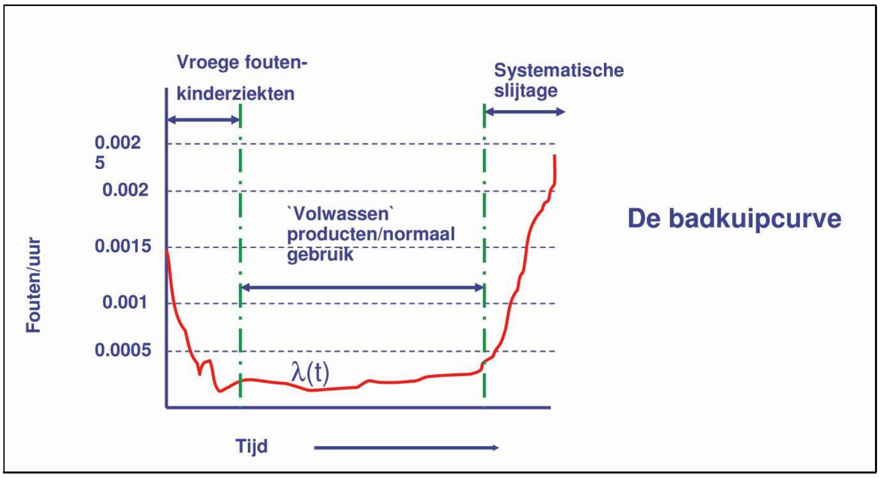
W1	Very Slight
W2	Slight
W3	Relatively High

-Figure 5 Risk graph

Failure probability λ:

The failure frequency is a measure of reliability that reflects the number of failures per unit of time of a number of (instrumental) components that have been deployed and are therefore exposed to failure.

The failure frequency of a component is high in the beginning due to teething problems. This decreases over time during normal use and then increases due to wear and tear. The failure frequency curve then looks like this:



-Figure 6 Bathtub curve

The failure probability λ is now defined as follows:

λ tot = failure of a component per unit time

λ tot consists of the following parts:

λ safe = probability of failure of components that lead to a safe condition

λ dangerous = probability of failure of components leading to a dangerous condition

It therefore follows that:

λ tot = λ safe + λ dangerous

These different failure probabilities can be further subdivided into λ d = detected failure probabilities (detected) and λ u = undetected failure probabilities (undetected).

The failure probabilities can now be graphically classified as follows: