




Definition of Safety Integrity Levels and the Influence of Assumptions, Methods and Principles Used

H. Schäbe

TÜV InterTraffic, Am Grauen Stein, 51105 Köln, Germany

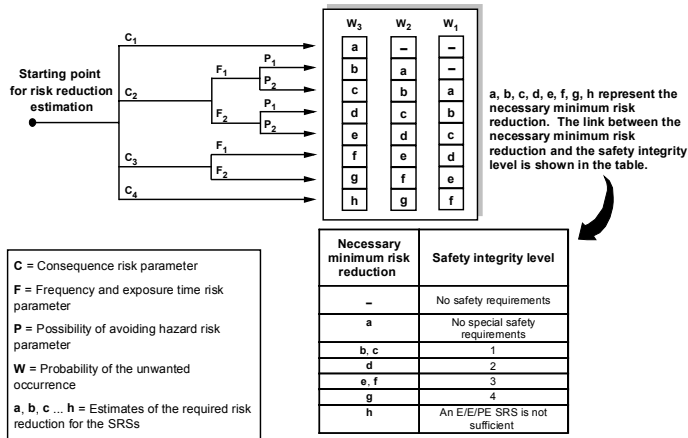
■ Introduction

- Methods for derivation of Safety Integrity Levels
- Minimum Endogeneous Mortality (MEM) 
- As Low As Reasonably Practicable (ALARP),
- Globalement Aussi Équivalent (GAME), 
- IEC 61508 risk graph 

Study of different principles and comparison

■ Safety Integrity Level Definition – IEC 61508

- Risk Graph from IEC 61508



■ Safety Integrity Level Definition – IEC 61508

Risk parameter	Classification
Consequence (C)	C ₁ Minor injury C ₂ Serious permanent injury to one or more persons; death to one person C ₃ Death to several people C ₄ Very many people killed
Frequency of, and exposure time in, the hazardous zone (F)	F ₁ Rare to more often exposure in the hazardous zone F ₂ Frequent to permanent exposure in the hazardous zone
Possibility of avoiding the hazardous event (P)	P ₁ Possible under certain conditions P ₂ Almost impossible
Probability of the unwanted occurrence (W)	W ₁ A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely W ₂ A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely W ₃ A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely

■ SIL Definition MEM and GAME

Minimum Endogenous Mortality

A new technical system must not add an unjustifiable amount of risk to the risk budget of a person. The starting point is the endogenous mortality of a 15-20 year old human being. Considering only endogenous fatality causes, this is a rate of $2 \cdot 10^{-4}$ / year.

GAME principle

A new technical system shall be globally be at least as good as the old one,

■ Tolerable Rates of Dangerous Failures and SILs

Safety Integrity Level	Rate of Dangerous Failures
SIL 1	$10^{-6}/h \dots < 10^{-5}/h$
SIL 2	$10^{-7}/h \dots < 10^{-6}/h$
SIL 3	$10^{-8}/h \dots < 10^{-7}/h$
SIL 4	$10^{-9}/h \dots < 10^{-8}/h$

■ Example – Track Worker Warning System

Risk graph

Parameters: C3 (since several people can be killed when the track worker crew is not warned.), F2 (since the persons are frequently in the dangerous zone), W2 or W3.

Result: SIL 3 or SIL 4

MEM

The risk of a single technical system shall not exceed $10^{-9}/h$.

Assuming that only in 20% of the failure of the track worker warning system will lead to accidents.

Result: rate of dangerous failures is $5 \cdot 10^{-9}/h$, yielding SIL 4.

■ Example – Track Worker Warning System

GAME

- a) watch-out (optimistic version)
- b) simple, single watch-out (pessimistic version)
- c) occupational health.

■ GAME

a) *watch-out (optimistic version)*

A single track worker is dedicated.

Two signals given. Probability for human failures of $5 \cdot 10^{-4}$.

Assume 2 trains per hour.

Result: $2 \cdot (5 \cdot 10^{-4})^2 / h = 5 \cdot 10^{-7} / h$ giving SIL2.

b) *simple, single watch-out (pessimistic version)*

Single track worker

One failure of watch out leads to accident.

Two trains per hour.

Result: $2 \cdot 5 \cdot 10^{-4} / h = 10^{-3} / h$ giving SIL 0.



■ GAME

c) *Occupational health*

Inputs:

- Kuhlmann gives a target for construction workers of $2 \cdot 10^{-7} / h$. R

-Railway Safety reports an average rate of 3 fatalities per 20000 workers per year, giving a rate of $3 / (20000 \cdot 1500h) = 10^{-7} / h$, assuming 1500 working hours per year.

Result: rate of $2 \cdot 10^{-7} / h$ or $10^{-7} / h$ giving SIL 2.



■ Results

Principle	SIL
IEC 61508	SIL 3 / SIL 4
MEM	SIL 4
GAME: watch out (optimistic versions)	SIL 2
GAME: watch out (pessimistic version)	SIL 0
GAME: occupational health	SIL 2

■ Conclusions

- Results of the different approaches applied to the example mainly coincide.
- More stringent requirements also lead to a higher SIL.
- The highest SIL comes from the requirement that the level of safety for a track worker should be the same as in normal life, i.e. application of the MEM principle.
- The lowest SIL is obtained as a result of the requirement that the system should be as good as a controller of site safety under very pessimistic assumptions.
- Other approaches give intermediate results.
- The result obtained from the risk graph fits into the range of other results.