Reliability data needs for functional safety analysis

Stefan L. Isaksen, Principal Adviser (Safetec)

and ISO/TC67/WG4 Committee Member

5th ISO Seminar on International Standardization in the Reliability Technology and Cost Area

Hosted by TotalEnergies, Paris, France - 1 December 2022

Reliability data collection – simplistic view

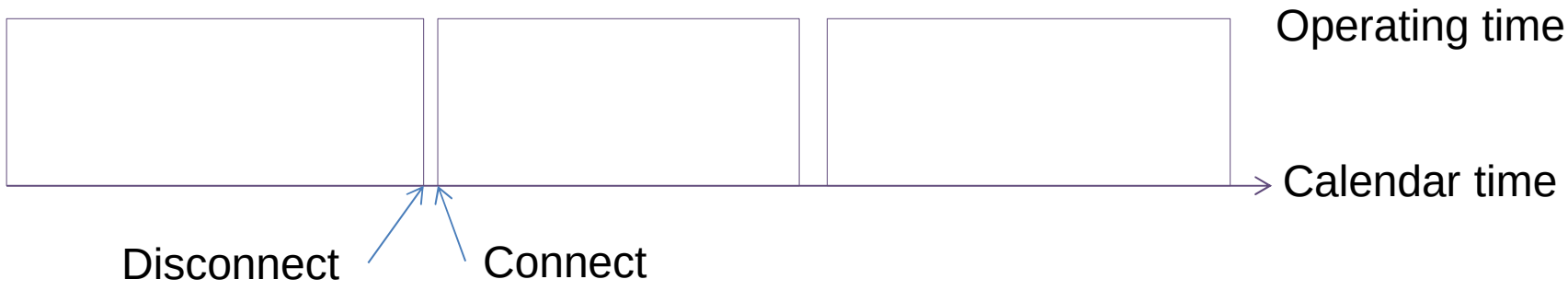
- Define data collection period
- Register number of failures
- Assume exponential distribution
- Divide number of failures by time to get the failure rate

Reliability data collection – complex issues

- Define data collection period (Calendar time/operational time? Degree/rate of use? Hot/cold standby? Etc.)
- Register number of failures (Critical/degraded/incipient failures? Failure modes, mechanisms and causes. Failure detection issues. Etc.)
- Assume exponential distribution (Validity of assumption?)
- Divide number of failures by time to get the failure rate (What if time is not the driving factor?)

Failure rate calculation – illustrative example

- Wellhead/XT connection MTTF ~500 years (operating/calendar time)



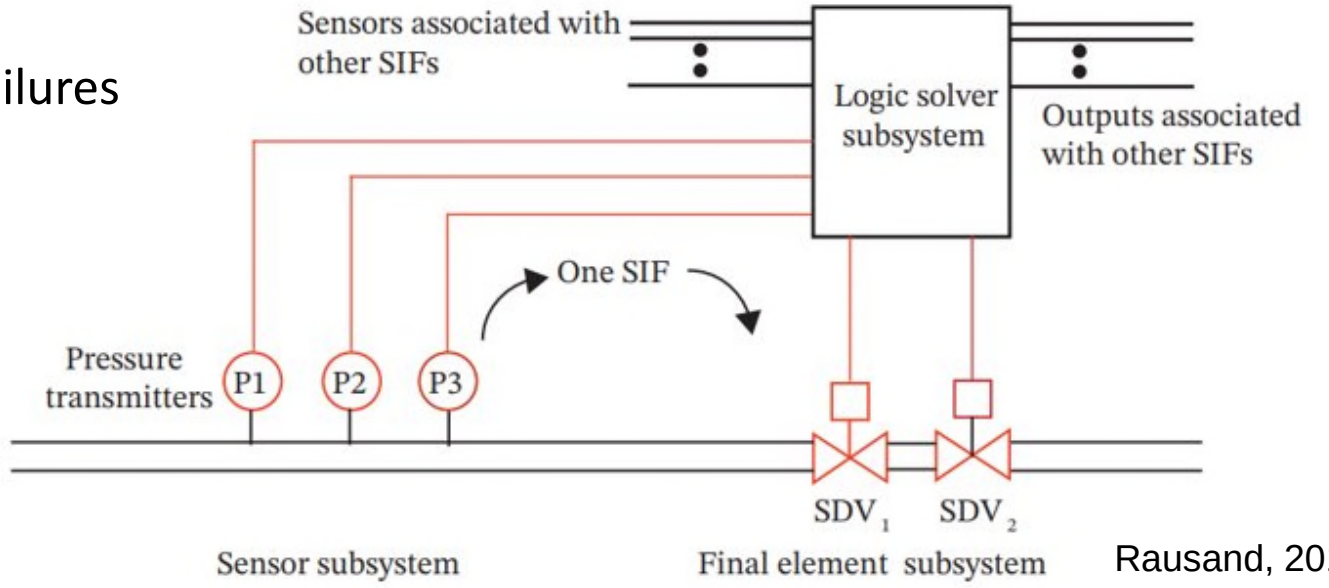
- Wellhead/BOP connection MTTF ~3 years (operating time)

Time factor vs. usage factor

- Failure modes and failure mechanisms/causes
  - Valve failure to open -> Corrosion (time issue)
  - Valve failure to open -> Wear (cycles issue)
- More information collected -> more flexibility in later analyses
- Appropriate reliability metric?
  - Mean Time To Failure (MTTF)
  - Mean Cycles To Failure (MCTF)
  - Probability of failure on demand (PFD)

Characteristic challenges for safety equipment

- Much stand-by time and testing
- Test demands and operational demands
- More complex failure detection (ISO 14224, Table B.4)
- Data pertaining to the SIL-calculations
  - Dangerous and safe failures
  - Detected and undetected failures
  - Diagnostic coverage
  - Demand rate



Rausand, 2014

Important additions in ISO 14224:2016

C.3.4 Failure as function of cycles rather than time

Table 5

Operation (normal use)	Normal operating state/ Mode (*)	6	Running	Active stand-by	Intermittent	Running
	Initial equipment commissioning date	6	2003.01.01	2003.01.01	2003.01.01	2003.01.01
	Start date of current service (*)	6	2003.02.01	2003.02.01	2003.02.01	2003.02.01
	Surveillance time, h (calculated) (*)	6	8 950	8 000	5 400	26 300
	Operational time, h [d] (measured/calculated)	6	7 540	675	2 375	22 870
	Number of periodic test demands during the surveillance period as applicable (*)[e]	6 - 8	4	2	2	4
	Number of operational demands during the surveillance period as applicable (*)[e]	6 - 8	4	5	11	3
	Total wells drilled during surveillance period (*)[f]	4	42	N.A.	N.A.	N.A.
	Operating parameters as relevant for each equipment class, e.g. ambient conditions, operating power (see Annex A)	6	Equipment-specific	Equipment-specific	Equipment-specific	Equipment-specific

Table 6

Data category	Data to be recorded	Description
Identification	Failure record (*)	Unique failure record identification
	Equipment identification/Location (*)	E.g. tag number (see Table 5)
Failure data	Failure date (*)	Date of failure detection (year/month/day)
	Failure mode (*)	Usually at equipment-unit level (level 6) (see B.2.6) [a]
	Failure impact on plant safety (e.g. personnel, environment, assets) [b]	Qualitative or quantitative failure consequence categorization (see also C.1.10)
	Failure impact on plant operations (e.g. production, drilling, intervention) [b]	Qualitative or quantitative failure consequence categorization (see also C.1.10)
	Failure impact on equipment function (*)	Effect on equipment-unit function (level 6): critical, degraded, or incipient failure [c]
	Failure mechanism	The physical, chemical or other processes which have led to a failure (see Table B.2)
	Failure cause [d]	The circumstances during design, manufacture or use which have led to a failure (see Table B.3)
	Subunit failed	Name of subunit that failed (see examples in Annex A)
	Component/Maintainable item(s) failed	Name of the failed component/maintainable item(s) (see Annex A)
	Detection method	How the failure was detected (see Table B.4)
	Operating condition at failure (*)	Run-down, start-up, running, hot standby, idle, cold standby, testing
	Operational phase at failure [e]	Type of operation at the time of failure
	SIS failure mode classification [f]	Classify the failure for the specific event (DU, DD, SU, SD; see F.2) [g]
Remarks	Additional information	Give more details, if available, on the circumstances leading to the failure: failure of redundant units, failure cause(s) etc.

[a] For some equipment categories such as subsea equipment, it is recommended to also record failure modes on taxonomic levels lower than the equipment-unit level.

[b] See example of failure consequence classification in Table C.2

[c] For some equipment categories and applications it may be sufficient to record critical and non-critical (degraded + incipient) failures only.

[d] The failure cause and sometimes the failure mechanism are not known when the data are collected, as they commonly require a root cause analysis to be performed. Such analysis shall be performed for failures of high consequence, high repair/down time cost, or failures occurring significantly more frequent than what is considered "normal" for this equipment unit class ("worst actors").

[e] Relevant for some equipment, e.g. drilling, completion and workover equipment. The code table depends on equipment category. The operation at the time of failure should be specified, such as drilling, tripping, cementing, perforating, well killing, etc.

[f] This is for data collection purposes internally for the company and for applications on the specific installation where it is collected. Carefulness if generalizing due to possible differences in classification for the same equipment class on same or different installations.

[g] The classes, DU (dangerous undetected), DD (dangerous detected), SU (safe undetected), SD (safe detected), are defined in IEC 61508-4:2010. See also ISO/TR 12489:2013.

(*) Indicates the minimum data that shall be collected.

Experiences from data collection within functional safety

- Challenges related to reporting of failures and test results. Lack of understanding among maintenance personnel
  - Challenges related to assigning failures to the right part of the Safety Instrumented Function (SIF)
  - Registering test results «as left», instead of «as is»
- «Neglected» equipment, such as control logic units (Logic solvers and I/O equipment)
- Lacking information on detection method
- Lacking information on demand rates

Conclusions

- Quality generally over quantity but there is always a need to find the right balance
- Safety critical equipment often has different reliability data needs
  - Demands
  - DU/DD/SU/SD
  - Diagnostic coverage
- Be aware of underlying assumptions

Thank You / Questions?