Modelling degradations, condition based maintenance and imperfect tests for Safety Instrumented System

Anne Barros - Nicolas Lefebvre

NTNU / DNV-GL

February 10, 2017

Problem statement

Framework of Safety Instrumented Systems in low demand rates (Rausand 2014)

- Multi unit system
- Periodic inspections
  - Proof tests every τ
  - Partial tests every Δ
- Condition monitoring
  - Some units are continuously monitored
  - Some are inspected
  - Some are not monitored
- Maintenance
  - Renewal every τ
  - Other interventions possible every Δ

Problem statement

Current performance indicator

- Average availability between 2 proof tests
- Safety Integrity Level

Current more common assumptions for analytical formula

- Exponential lifetime law for all the units
- Perfect repair if failure detected at partial test
- No action if no failure detected
- No time to repair

Problem statement

Questions

- Should we consider other lifetime laws?
- Should we consider degraded states?
- Should we consider imperfect maintenance actions, preventive maintenance, optimisation?
- Should we consider the negative effect of tests (damage) of their performances (non detection, false alarm)?
- Should we consider time to repair?

Generic structure

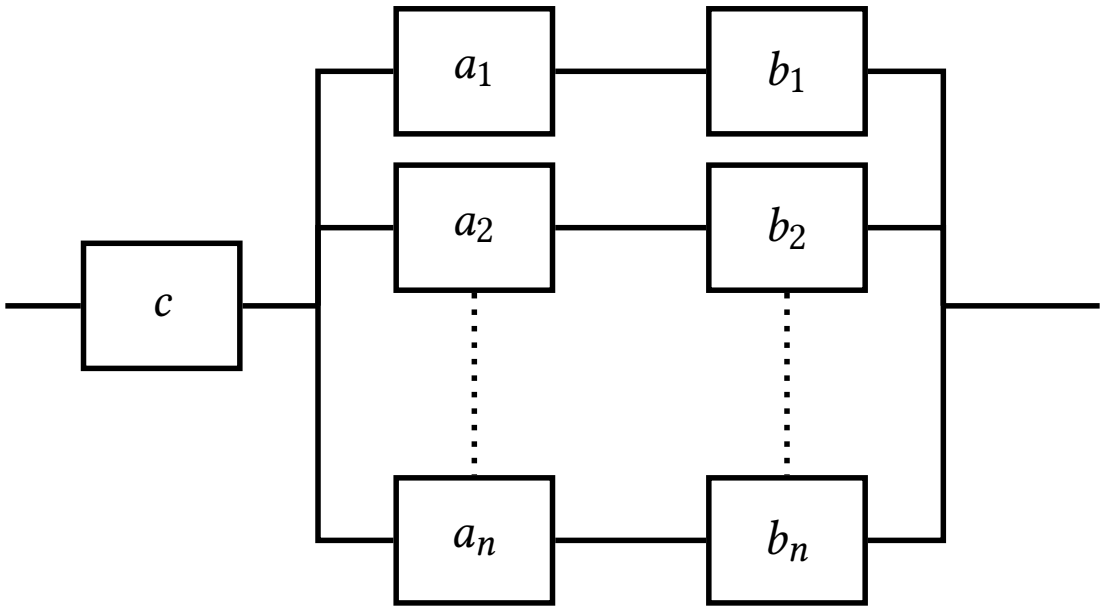


Figure: System reliability block diagram of a SIS with n channels

There are n channels and their state is denoted $\eta = (\eta_1, \ldots, \eta_n)$ with $\eta_i = 1$ if channel i is in the functioning state and $\eta_i = 0$ if it is failed. We note $\mathcal{M}$ the set of the functioning states for the redundant part of the system.

Some notations

We use notation of (Jin & Rausand 2014).

Each channel i ($1 \leq i \leq n$) can have two types of failures that can be modelled by two series units (with indexes a and b respectively).

These two units have a survival function noted $R_a(t)$ and $R_b(t)$.

The series unit has a constant failure rate λ_c.

All the time to failure are supposed to be independent.

Partial inspections (partial tests) are performed every Δ unit of time, at times $t_1, t_2, \ldots, t_{m-1}$ with $t_k = k\Delta$ and $\tau = m\Delta$.

What we can do

The time to repair unit a, b, c can be taken into account as a constant value m_a, m_b, m_c. Here only $m_c \neq 0$

During these partial tests, failure modes a can be detected with some imperfectness (unit a degraded due to the testing procedure or non detection)

A failure of unit c is supposed to be immediately detected due to embedded self-diagnosis functions.

Different kind of maintenance actions can then be planned. They can correspond to systematic complete renewal, renewal in case of failure or partial renewal.

Availability is calculated between each proof test before average calculation.

Other way to say the same thing

What is the RUL of the SIS until the next partial test? Not so easy to calculate.

What is the quality of the diagnosis and its impact on the system (destructive control) at each partial test? What it the impact of this quality on the SIS performance? Is condition monitoring meaningful?

What is the optimal inspection period?

Modelling

What we can calculate is the availability of the SIS at each time until the next partial test and the average availability in this interval

$$A(t) = A_c(t) \sum_{\eta \in \mathcal{M}} \prod_{i=1}^{n} (A_i(t))^{\eta_i} (1 - A_i(t))^{1-\eta_i} \tag{1}$$

The problem now is to calculate the availability $A_i(t)$ for each channel. If $t \in [t_{k-1}, t_k[$ for $k = 1, 2, \ldots, m$:

$$A_i(t) = R_b(t)\, A_a(t) \tag{2}$$

where $A_a(t)$ is the availability of indexed unit a at time t. It depends on degradation modelling, and maintenance policy.

Modelling

- One model based on virtual age

- One model based on degradation states

Virtual Age

If the unit a is functioning at time t_k and its age is $d\Delta$, then after the partial maintenance, its age is $f(d)\Delta$. The function f is a decreasing/increasing function defined from $[0, 1, \ldots, m-1]$ to $[0, 1, \ldots, m-1]$. If it is failed, it is supposed to be renewed.

Two extreme cases exist:

- if $f(d) = d$, it means that if the unit is functioning at the partial test, then nothing is done
- if $f(d) = 0$ for any d, it means that the part of the channel corresponding to unit a is completely renewed

Virtual Age

To calculate $A_a(t)$ we need to describe the evolution of the age of unit a. We introduce the Markov chain X_k which takes values between 0 and $m-1$ such that $X_k\Delta$ is the age of the unit at time $t_k = k\Delta$ $(0 \leq k \leq m-1)$. Then $X_0 = 0$ and for $0 \leq k \leq m-1$:

$$\mathbb{P}(X_k = f(d+1)/X_{k-1} = d) = \frac{R_a((d+1)\Delta)}{R_a(d\Delta)} \tag{3}$$

$$\mathbb{P}(X_k = 0/X_{k-1} = d) = 1 - \frac{R_a((d+1)\Delta)}{R_a(d\Delta)} \tag{4}$$

If we note M the transition matrix of this Markov chain, we obtain the column vector P_k of components $(\mathbb{P}(X_k = d),\ 0 \leq d \leq m-1)$ with : $P_k = M^k P_0$. Then if $t \in [t_k, t_{k+1}[$ $(0 \leq k \leq m-1)$, we can write:

$$A_a(t) = \sum_{d=0}^{m-1} \frac{R_a(t - t_k + d\Delta)}{R_a(d\Delta)} \mathbb{P}(X_k = d) \tag{5}$$

In case of the system is renewed at each partial test, we get $\mathbb{P}(X_k = 0) = 1$ and $A_a(t) = R_a(t - t_k)$.

Virtual Age

If $N(\eta)$ is the number of channels which are functioning when the system is in the functioning state η, then the availability is:

$$\begin{aligned} A(t) &= A_c(t) \sum_{\eta \in \mathcal{M}} \left(R_b(t)A_a(t)\right)^{N(\eta)} \left(1 - R_b(t)A_a(t)\right)^{n-N(\eta)} \\ &= A_c(t) \sum_{\eta \in \mathcal{M}} \sum_{j=N(\eta)}^{n} (-1)^{j-N(\eta)} C_{n-N(\eta)}^{j-N(\eta)} \left(R_b(t)A_a(t)\right)^j \end{aligned} \tag{6}$$

We can get an expression for the average availability over $[0, \tau[$ per unit of time (commonly named Probability of Failure on Demand - PFD):

$$\begin{aligned} \tilde{A}_\tau &= \frac{1}{\tau} \int_0^\tau A(s)ds \\ &= \frac{e^{-\lambda_c m_c}}{\tau} \sum_{i=1}^{m} \sum_{\eta \in \mathcal{M}} \sum_{j=N(\eta)}^{n} (-1)^{j-N(\eta)} C_{n-N(\eta)}^{j-N(\eta)} \int_{t_{i-1}}^{t_i} \left(R_b(s)A_a(s)\right)^j ds \end{aligned} \tag{7}$$

Exponential case

As a reference case, we can look at the case when the lifetime laws of units a and b are modelled by exponential laws with parameters λ_a and λ_b. Then, all the maintenance policies are equivalent to complete renewal at each partial test (systematic renewal). We have $R_a(t) = \exp(-\lambda_a t)$ and $R_b(t) = \exp(-\lambda_b t)$.

The analytical expression of the average availability is:

$$\tilde{A}_\tau = \frac{e^{-\lambda_c m_c}}{\tau} \sum_{\eta \in \mathcal{M}} \sum_{j=N(\eta)}^{n} (-1)^{j-N(\eta)} C_{n-N(\eta)}^{j-N(\eta)} \frac{1}{j(\lambda_a+\lambda_b)} \frac{e^{-j\lambda_b m\Delta} - 1}{e^{-j\lambda_b \Delta} - 1} \left(e^{-j(\lambda_a+\lambda_b)\Delta} - 1 \right)$$

For example if the system is made of two parallel channels, we get if $t \in [t_k, t_{k+1}[$:

$$\begin{aligned} A(t) &= e^{-\lambda_c m_c} \left((A_1(t))^2 + 2A_1(t)(1 - A_1(t)) \right) \\ &= e^{-\lambda_c m_c} (2A_1(t) - A_1^2(t)) \\ &= e^{-\lambda_c m_c} (2e^{-\lambda_b t - \lambda_a (t-t_k)} - e^{-2\lambda_b t - 2\lambda_a (t-t_k)}) \end{aligned} \tag{8}$$

and

$$\tilde{A}_\tau = 2 \frac{e^{-\lambda_c m_c}}{m\Delta} \frac{1 - e^{-m\lambda_b \Delta}}{1 - e^{-\lambda_b \Delta}} \frac{1 - e^{-(\lambda_a+\lambda_b)\Delta}}{\lambda_a + \lambda_b} - \frac{e^{-\lambda_c m_c}}{m\Delta} \frac{1 - e^{-2m\lambda_b \Delta}}{1 - e^{-2\lambda_b \Delta}} \frac{1 - e^{-2(\lambda_a+\lambda_b)\Delta}}{2(\lambda_a + \lambda_b)} \tag{9}$$

Weibull lifetime laws with general renewals

Lifetime of units a and b are Weibull laws with parameters λ_a, k_a and λ_b, k_b.
The matrix M equals for $0 \leq d \leq m-2$:

$$M(d, f(d+1)) = \exp\left(-(\lambda_a \Delta)^{k_a}((d+1)^{k_a} - d^{k_a})\right)$$
$$M(d, 0) = 1 - M(d, f(d+1)) \tag{10}$$

and $M(m-1, 0) = 1$.
Then for $t \in [t_{k+1}, t_k[$ $(0 \leq k \leq m-1)$,

$$A_a(t) = \sum_{d=0}^{m-1} \frac{e^{-(\lambda_a(t-t_k+d\Delta))^{k_a}}}{e^{-(\lambda_a(d\Delta))^{k_a}}} (M^k P_0)(d+1, 1) \tag{11}$$

and the system availability is:

$$A(t) = e^{-\lambda_c m_c} \sum_{\eta \in \mathcal{M}} \left(e^{-(\lambda_b t)^{k_b}} A_a(t)\right)^{N(\eta)} \left(1 - e^{-(\lambda_b t)^{k_b}} A_a(t)\right)^{n-N(\eta)} \tag{12}$$

$$= e^{-\lambda_c m_c} \sum_{\eta \in \mathcal{M}} \sum_{j=N(\eta)}^{n} (-1)^{j-N(\eta)} C_{n-N(\eta)}^{j-N(\eta)} \left(e^{-(\lambda_b t)^{k_b}} A_a(t)\right)^{j} \tag{13}$$

Weibull lifetime laws with general renewals

In case of two channels, we get:

$$A(t) = e^{-\lambda_c m_c} \left(2e^{-(\lambda_b t)^{k_b}} A_a(t) \left(1 - e^{-(\lambda_b t)^{k_b}} A_a(t) \right) + \left(e^{-(\lambda_b t)^{k_b}} A_a(t) \right)^2 \right) \tag{14}$$

The average availability over $[0, \tau[$ equals:

$$\frac{1}{\tau} \int_0^\tau A(s)\, ds \quad = \quad \frac{e^{-\lambda_c m_c}}{\tau} \sum_{i=1}^{m} \sum_{\eta \in \mathcal{M}} \sum_{j=N(\eta)}^{n} (-1)^{j-N(\eta)} \, C_{n-N(\eta)}^{j-N(\eta)} \int_{t_{i-1}}^{t_i} \left(e^{-(\lambda_b s)^{k_b}} A_a(s) \right)^j ds$$

Numerical results

Numerical results are limited for this paper to two channels in parallel.

For reminder:

- a failure of component c is immediately detected and followed by a corrective maintenance.
- failures of component b are not detected.
- after one inspection (partial test), component a is instantaneously renewed if it is failed at the inspection time

Numerical results

In our modelling framework, the matrix M allows the modelling of different preventive maintenance policies for unit a. It can be decided to put unit a back to any age $d\Delta$ lower than the current one. Numerical results focus here on a special case: when unit a is found to be working at one inspection, nothing is done and when unit a is found to be failed at one inspection, it is replaced by a new one. This is a maintenance policy currently applied to many SIS in low demand mode.

We focus here on a discussion about Weibull law versus exponential one.

Numerical results

We consider the framing condition given by data bases as OREDA (SINTEF, NTNU, & DNV-GL 2015). This data basis gives for each unit of the SIS an estimation of the mean number of failures per unit of time. Usually, this mean is used by fitting an exponential lifetime distribution. We propose here to fit several possible Weibull distributions and then to use our virtual age model to calculate the system availability. The objective is to show that starting with the same inputs but with different assumptions for the lifetime model, we can obtain significant variations for the availability and the average availability between two proof tests. We focus on component a because it is the one that can be maintained at test/inspection times. Hence, the common assumption of exponential distribution can be problematic because:

- if we want to increase the inspection periods, we should be able to push the unit to be out of the zone of "constant failure rate" and to evaluate the impact of an increasing failure rate,
- it can be unrealistic to assume that the tests and renewals are always perfect and make the unit systematically back to an as good as new state.

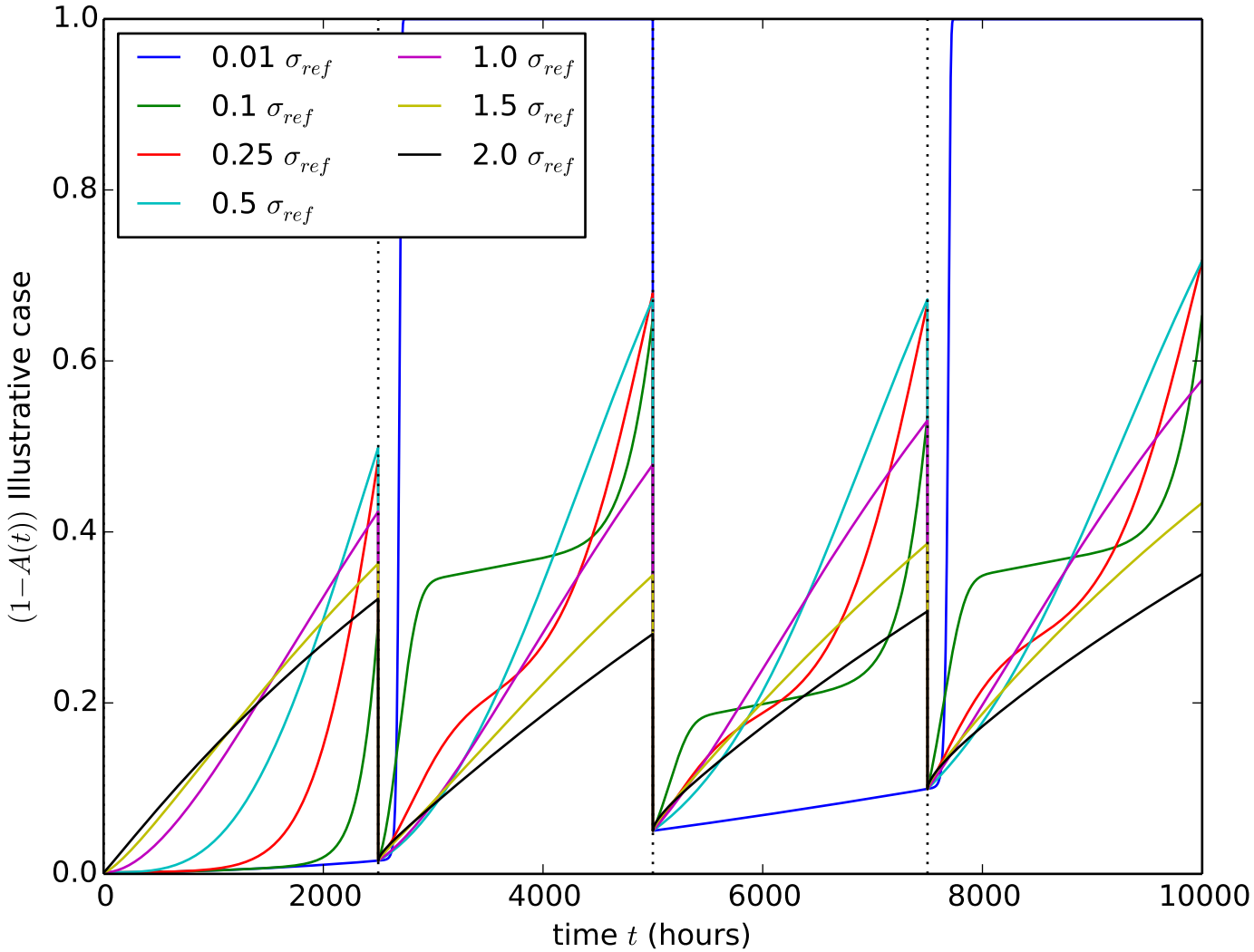
Numerical results

With exponential law, the average value of component a is $\mu_{ref} = 1/\lambda_a$ and the standard deviation is $\sigma_{ref} = 1/\lambda_a$. If we consider that the component a follows a Weibull law with parameters (λ_a, k_a) and it has the same mean as the exponential one, then the parameters λ_a and k_a have to be tuned in such a way that the resulting μ_{ref} is kept equal to the exponential case and the standard deviation is equal to $K\,\sigma_{ref}$ where the coefficient K can take the following values $[0.01, 0.1, 0.25, 0.5, 1, 1.5, 2]$. The resulting distributions are represented through histograms.

Numerical results

Illustrative set of parameters: the total renewal and inspection periods are respectively: $\tau = 10000, \Delta = 10000/4$, $m = 4$. Components a, b and c follow exponential laws with parameters $\lambda_a = 1/2700, \lambda_b = 1/20000, \lambda_c = 1/5000$. The duration of the corrective maintenance of component c is $m_c = 8$.

Numerical results



Numerical results

Table: Illustrative set of parameters

K	λ_a	k_a	$1-\tilde{A}$
0.01	3.7203e-04	127.5302	4.8499e-01
0.10	3.8631e-04	12.1534	2.4290e-01
0.25	4.0563e-04	4.5422	2.3790e-01
0.50	4.1817e-04	2.1013	2.7843e-01
1.00	3.7037e-04	1.0000	2.6327e-01
1.50	2.8638e-04	0.6848	2.2047e-01
2.00	2.1306e-04	0.5427	1.9138e-01

Numerical results

Realistic set of parameters: We consider a shutdown valve. Realistic input parameters given are: $\tau = 8760, \Delta = 8760/4, m = 4, \lambda_a = 0.52e-6, \lambda_b = 0.28e-6, \lambda_c = 6e-6, m_c = 8$ (Jin & Rausand 2014), (Rausand 2014), (Habrekke, Hauge, & Onshus 2013).

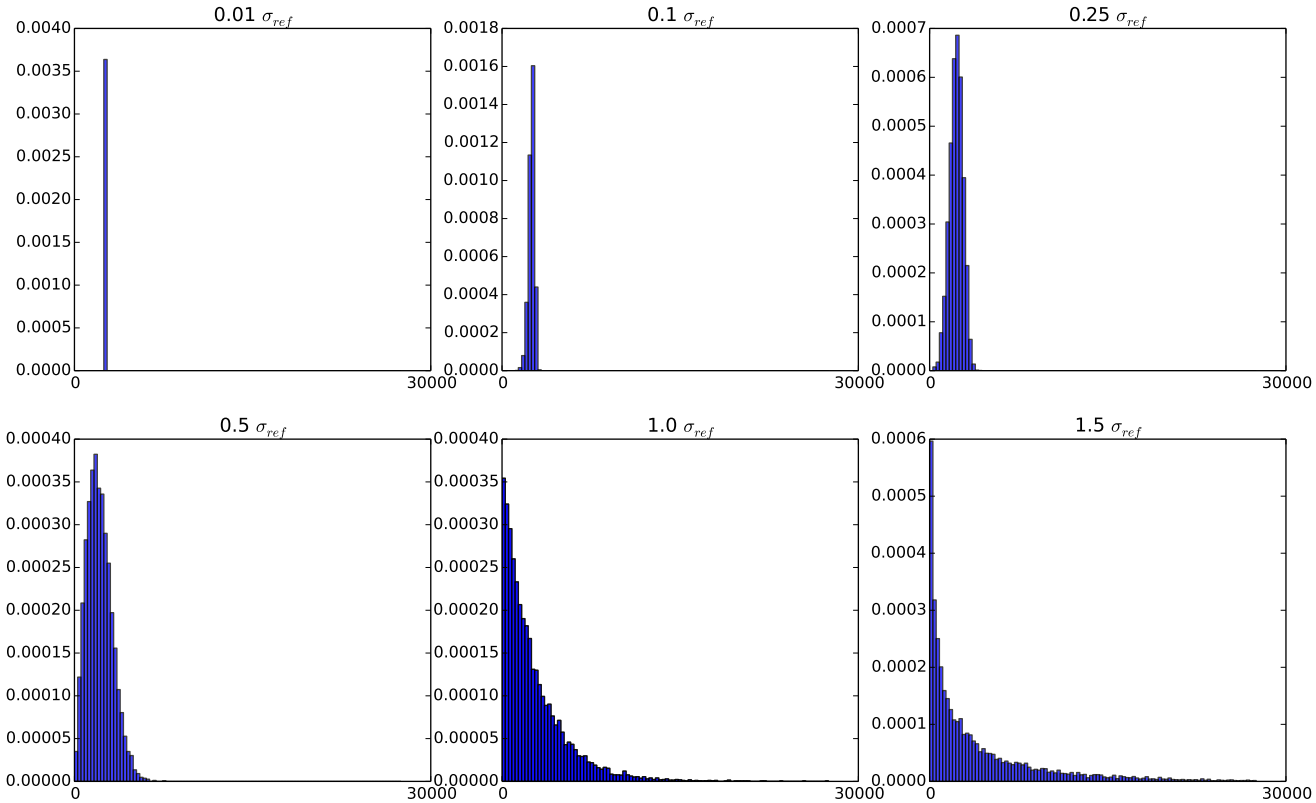


Figure: Histogrammes obtained with the same MTTF but different standard deviations for unit a

Numerical results

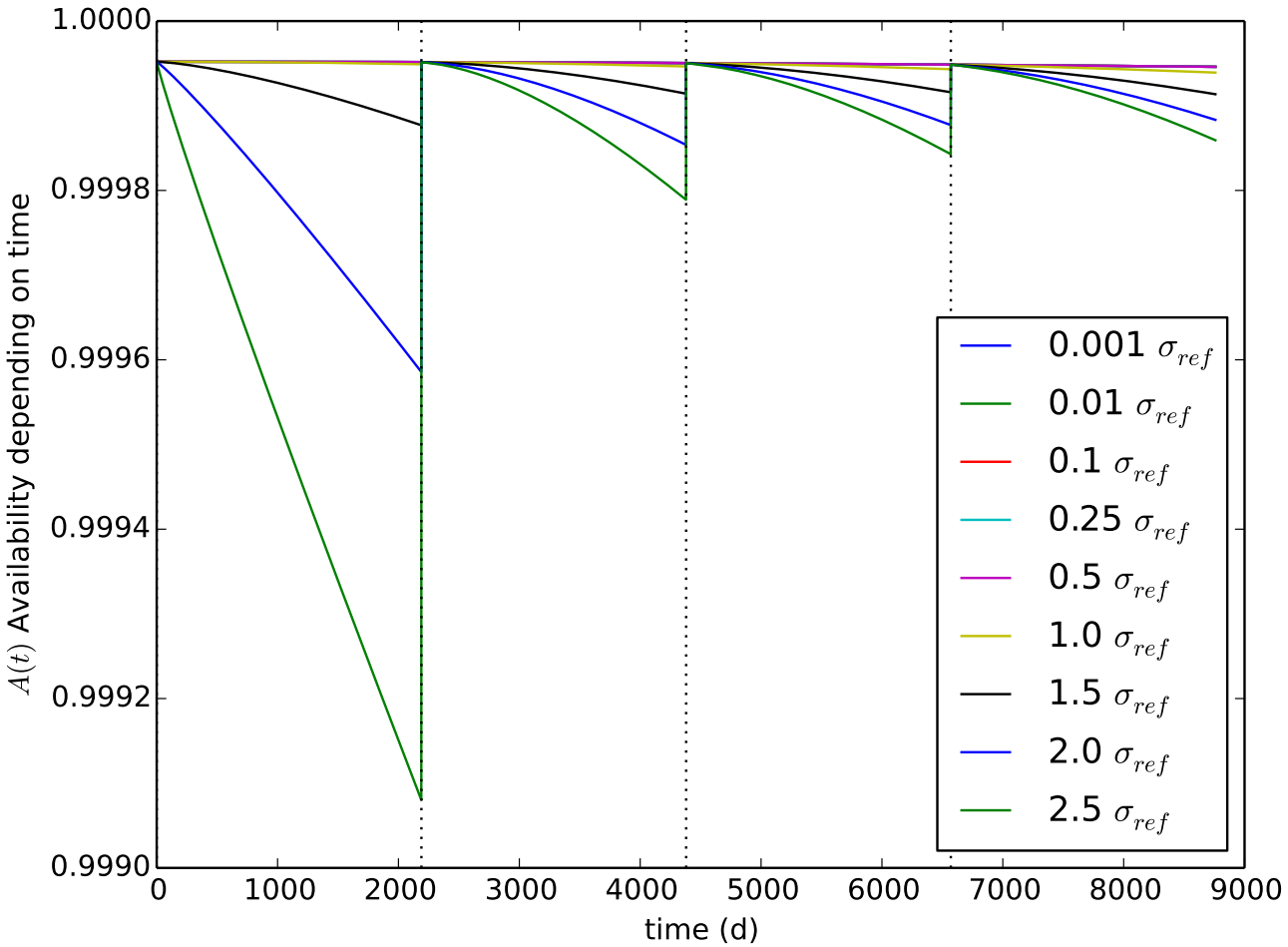


Figure: Availability for each partial test interval

Numerical results

We can notice that when K increases, the number of infant failure increases and this impacts accordingly the availability. On the opposite when K decreases, we can expect a reduction of the spreading of the failure dates around the average value which is in this case upper than the renewal period. Therefore, component a does not fail anymore and we obtain mostly the curve associated to the failures rates of components b and c. In Table 2, we can observe that the average unavailability $1 - \tilde{A}$ is constant for the smaller values of coefficient K. In these cases, there is almost no failure of the component a on the period $[0, \tau[$ therefore, the availability is "constant" and depend only on component b and c. Then, the availability decreases when the value of coefficient K increase: the probability of failure of the component a increases on the considered period $[0, \tau[$ since the standard deviation of the distribution of the time to failure increases for a fixed average value.

Numerical results

K	λ_a	k_a	$1-\tilde{A}$
0.01	5.2233e-07	127.5302	5.0000e-05
0.10	5.4238e-07	12.1534	5.0000e-05
0.25	5.6951e-07	4.5422	5.0000e-05
0.50	5.8711e-07	2.1013	5.0006e-05
1.00	5.2000e-07	1.0000	5.1938e-05
1.50	4.0208e-07	0.6848	6.7778e-05
2.00	2.9913e-07	0.5427	1.1606e-04

Table: Average unavailability for different values of the standard deviation

Numerical results

The change of assumption for the lifetime law can affect the Safety Integrity Level (SIL) in some extreme cases. According to the IEC 61508 standard (**?**), a SIS has a SIL 4 if its mean unavailability per unit of time is in $[10^{-5}, 10^{-4}]$. Regarding Figure 4 and Table 2, it is clear that the SIL of our realistic system can be affected by the lifetime assumption. Then from a safety point of view, the exponential law can be reasonable or not. It depends on the standard deviation among the failure dates and also on the period inspections. Here we can see that only a very high standard deviation can influence the SIL if it is inspected every 2500 hours. We study now the impact of the inspection periods on the average unavailability for different values of K.

Numerical results

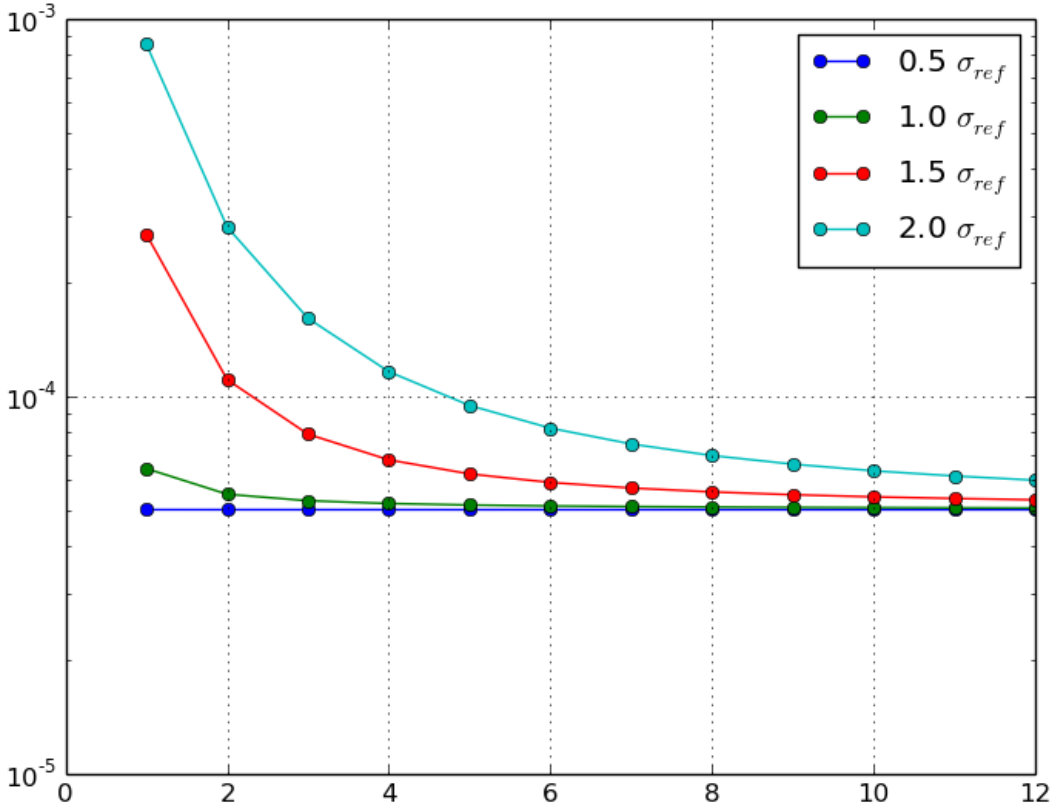


Figure: Unavailability according to the number of partial test per year

$\tau = 8760h, MTTF_a = 1923076h, MTTF_b = 3571428h, MTTF_c = 166666h, m_c = 8h$

Numerical results

When the number of partial test is high, the system unavailability is weakly impacted by larger standard deviation of the time to failure. The impact is much more important when the number of partial tests is lower.

Discussion about OREDA

Conclusion

Further work will be devoted to:

- investigation for other realistic data sets and impact on the Safety Integrity Level,
- numerical analysis for intermediate cases when the age of unit a can be reduced or increased by partial repair at inspection/test date,
- use of more advanced framing condition for the data set. We expect at least to have the number of failures for each interval between to partial tests. Given that no preventive actions are currently done on working units, it is possible to capture in such data set some degradation trend and for example some information about the Weibull parameters.

Modelling

- One model based on virtual age

- One model based on degradation states (Generalised Markov Process)

Generalised Markov Process

The evolution of a type a unit between two maintenance interventions is modelled by a discrete states degradation process and the transition rates $\lambda_{a,k}$ from state k to state $k+1$, $(k = 0, 1, \ldots, K-1)$ are given by the following transition matrix:

$$A = \begin{pmatrix} -\lambda_{a,0} & \lambda_{a,0} & 0 & \ldots & 0 & 0 \\ 0 & -\lambda_{a,1} & \lambda_{a,1} & \ldots & 0 & 0 \\ 0 & 0 & -\lambda_{a,2} & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \lambda_{a,K-2} & 0 \\ 0 & 0 & 0 & \ldots & -\lambda_{a,K-1} & \lambda_{a,K-1} \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}$$

We are now looking at the system performance within the renewal time interval $[0, \tau[$.

Generalised Markov Process

During one inspection, units a can be renewed systematically, renewed if they are failed, or partially renewed.

In order to model this, we define a matrix M such that if the unit is in state k before the maintenance, it will be in state m after the maintenance with the probability $M_{k,m}$ ($\sum_{m=0}^{K} M_{k,m} = 1$).

If unit a is systematically renewed, then for any k $M_{k,0} = 1$ and $M_{k,m} = 0$ for $m \neq 0$. If the unit is renewed only when a failure occurs, then $M_{K,0} = 1$ and $M_{k,k} = 1$ for $k \neq K$. For a partial maintenance, all the cases can be considered.

Generalised Markov Process

In order to calculate $A_a(t)$, we describe the evolution of a type a unit.

If $t \in [t_k, t_{k+1}[$, the law μ_t of the unit state is:

$$\mu_t = \mu_0 \left(e^{\tau A} M\right)^k e^{(t-t_k)A}$$

and

$$A_a(t) = 1 - \mu_t(K) = 1 - \mu_0 \left(e^{\tau A} M\right)^k e^{(t-t_k)A}(K)$$

Generalised Markov Process

Habrekke, S., S. Hauge, & T. Onshus (2013).
Reliability Data for Safety Instrumented Systems.
SINTEF.

Jin, H. & M. Rausand (2014).
Reliability of safety-instrumented systems subject to partial testing and common-cause failures.
Reliability Engineering & System Safety 121, 146 – 151.

Rausand, M. (2014).
Reliability of Safety-Critical Systems: Theory and Applications.
Hoboken, NJ, USA: John Wiley & Sons.

SINTEF, NTNU, & DNV-GL (2015).
OREDA : offshore and onshore reliability data handbook.
OREDA Participants.