Die Fallstricke der Verfügbarkeit
(Trapped with availability)
Hendrik Schäbe
In railway development frequently the main focus is on safety. 
On the other hand, also availability is important. 
We will discuss availability problems: 
  - The role of availability, 
  - We show what the railway standard EN 50126 requires for availability 
  - We provide some information on statistical methods.
For many railway systems, the primary focus is on safety. However, an insufficient level of availability can also cause safety problems.

Assume a safety system as e.g. an interlocking must satisfy a tolerable hazard rate of \( \lambda \), e.g. \( 10^{-8}/h \). This system is now available with an availability of \( A \).

If the system is unavailable, a fall-back solution with a rate of dangerous failure \( \lambda_f \) is applied.

\[ \lambda A + \lambda_f (1-A) \]
- Ensure that safety is not corrupted by bad availability
  - \( \lambda_f (1 - A) < \lambda \),
  - Possibility 1:
    - \( A > 1 - \frac{\lambda}{\lambda_f} \)
  - Possibility 2:
    - \( \lambda_f < \frac{\lambda}{1 - A} \).

- Example:
  - target rate of dangerous failures of \( 10^{-8} \)/h
  - fall-back solution has a rate of \( 10^{-4} \)/h, the availability of the system must be 0.9999.
  - availability of the system is 0.999, the fall-back solution provides must have \( \lambda_f = 10^{-5} \)/h.
  - BO Strab: emergency brake (false positives)
How to ensure a good availability?

- EN 50126 also defines a **RAM** process for the entire life cycle, besides a safety process.
- For RAM, an independent party is normally not asked for a RAM assessment.
- As a consequence, much less is done for RAM than for safety.
- In order to achieve a good RAM performance, guidance is given by EN 50126 and figure 9 gives the tasks to be carried out.
Phase 4 (System requirements)
Specify System RAM requirements
Define RAM acceptance criteria
Establish RAM programme and RAM management

The first two points can usually be found in the requirements specification. However, not all requirements might be clear and not all might be really practically applicable. The last point is often implemented incompletely, not only by small enterprises.
- Phase 5 (Apportionment of system requirements)
- Specification of subsystem RAM requirements and acceptance criteria
- Show that the system architecture is able to fulfil the RAM requirements and to substantiate this by quantitative analyses. This analysis should show, that the RAM parameters of the subsystem are able to guarantee that the system fulfils the RAM requirements.
Phase 6 (Design and implementation)

- Implement RAM programme
- EN 50126 clause 6.6.5.1
  - „e) verification, by analysis and test, that the manufacturing arrangements produce RAMS-validated sub-systems and components“.
  - Analyses must be carried out to show that maintainability aspects have been duly taken into account (corrective and preventive inspections)
  - Analysis to show that the RAM parameters will be achieved by the system (availability prediction)
  - RAM demonstration programme is implemented
- **Phase 7**
  - Environmental stress screening
  - RAM improvement testing
  - Commence FRACAS (Failure Reporting and Corrective Action System)

- **Phase 8 (Installation)**
  - Establish spare parts and tool provisions
The availability is (MIL-HDBK 472)

\[ A = \frac{MTBF}{MTBF + MDT}, \]

Where MTBF is the mean time between failures and MDT is the mean downtime.

MTBF and MDT are estimated from the observed data \( X_i, i=1,..n \) of times between system failures and \( Y_j, j=1,..m \), of system down times.

\[
MTBF_s = \frac{\sum_{i=1}^{n} X_i}{n},
\]

\[
MDT_s = \frac{\sum_{j=1}^{m} Y_j}{m},
\]
- Assume exponential distributions for the times between failures (motivated by many different fault processes and Grigelionis‘ theorem)
- Assume exponential distributions for downtimes (complicated, because the usual ansatz is log-normality, the author has, however also found data that are exponentially distributed due to many different failure causes)

Then a confidence interval would be:

\[
\left[\frac{1}{1 + MDTs F_{2m;2n}(1-\alpha/2)/MTBFs)}; \frac{1}{1 + MDTs F_{2m;2n}(\alpha/2)/MTBFs)}\right]
\]
Example for confidence intervals for availabilities, computed for small time intervals
Other approach

- Assume, the system has been observed for an overall time $T$ and $MDTs$ is the estimated mean down time calculated from the sample $Y_j$, $j=1,\ldots,m$.
- $n (MDT_s+MTBF_s) = T$, since there are as many downtimes as uptimes and all down and uptimes must sum up to the total observation time $T$.
- $A_s = MTBF_s / (MTBF_s + MDT_s) = (T - n MDT_s) / T$
- Confidence interval for the availability:
  - $[(T - 2n^2 MDT_s/\chi^2_{2n}(\alpha/2)) / T ; (T - 2n^2 MDTs/\chi^2_{2n} (1-\alpha/2)) / T]$.
- This confidence interval is conditional on the number of observed events (failures).
Use of a Chi-Square distribution for confidence intervals of the availability (two sided, 95% coverage)
Averaging availabilities?

- Compute
  \[ A_s = \frac{(A_{s,1} + \ldots + A_{s,r})}{r} \]
  as an estimate of \( r \) availability estimates.
- Is \( A_s \) unbiased, i.e. \( E(A_s) = A \)?
- Only if \( E(A_{s,i}) = A \) for all \( i \).
- What if this is not the case?
- Expanding the expectation of \( A \).
  \[ E(A_{s,1}) = A + v_x^2(A - 3A^2 + 2A^3)/n + 2A(1-A)^2v_y^2/m + \ldots, \]
  where \( v_x \) and \( v_y \) are the variational coefficients of \( X \) and \( Y \).
- Note that only for large \( m \) and \( n \) the mean of the estimator comes close to the true value. But: \( m \) and \( n \) are the sample size of a single estimator. Taking large \( r \) (averaging availability estimates) does not increase \( m \) or \( n \).
- Example: \( m = n, 1, \ldots, 4 \), variational coefficients of 0.25
Bias of averaged availability estimates
Exclusion to the rule

- Assume \( A_{s,i} = \frac{T-n_i \text{MDT}_{s,i}}{T}, i=1,..,r. \)
- Then
- \( A_s = \frac{A_{s,1} + A_{s,2} + \ldots + A_{s,r}}{r} = \frac{(rT - (n_1 \text{MDT}_{s,1} + n_2 \text{MDT}_{s,2} + \ldots + n_r \text{MDT}_{s,r}))}{rT} \)
- \( = \frac{(rT - n \text{MDT}_s)}{rT} \)
- since
- \( n \text{MDT} = n_1 \text{MDT}_{s,1} + n_2 \text{MDT}_{s,2} + \ldots + n_r \text{MDT}_{s,r} \)
- This is only true if the time intervals are the same.
Analysing trends

Evaluation of downtimes during the same time interval over time
- Carry out a statistical test for slope of the regression line according to e.g. Bickel and Docksum.

- **Analyse the number of failures.**
  - Use the Nonhomogeneous Poisson process (NHPP).
  - Cumulated number of events up to time \( t \) is \( t^{\beta/\Theta} \).
  - The NHPP is a transformed HPP with
    - \( t' = t^{\beta/\Theta} \)
    - \( \beta \) is estimated by
      - \( \beta_s = \sum \ln(t_i/T) \), where
      - \( \Sigma \) is a sum over all \( i \) from 1 to \( n \),
      - \( T \) is the time the process has been observed.
    - \( t_1 = X_1 \),
    - \( t_i = t_{i-1} + X_i \).
Now $2n \beta_s/\beta$ has a Chi-Square distribution with $2(n-1)$ degrees of freedom so that a confidence interval for $\beta$ is given by

$$[2n \beta_s /\chi^2_{2(n-1)}(\alpha/2); 2n \beta_s /\chi^2_{2(n-1)}(1-\alpha/2)].$$

These values can also be used as critical values to test the hypothesis $b>0$ (i.e. the number of failures is increasing which is not desirable) or $b<0$ (the number of failures is decreasing).

In a simulated example we have computed for $n=158$ events:

- $\beta_s = 0.496$
- $\Theta_s = 0.00319$
- and the confidence interval for $\beta$ with 90% coverage
- $[0.4396,0.5718]$. 
Number of failures and intensity of Nonhomogeneous Poisson process
Conclusions

- In this paper we have discussed problems connected with availability. We have shown that for RAM and availability a process comparable with the one for safety should be set up according to EN 50126 to achieve an available system.

- Moreover, estimation and statistical testing has been discussed. We have proposed two very simple methods to compute a confidence interval. It has been shown that availability estimates shall be computed from larger samples and that availability values for short time periods do not make sense.

- We have provided methods to investigate trends in availability.