Chapter 1.2

DEPENDABILITY EVALUATION METHODS
Classification

Tomislav Lovric

TÜV InterTraffic GmbH, Am Grauen Stein, D-51105 Köln - Germany

1. TYPES OF DEPENDABILITY EVALUATION METHODS

Dependability, the ability of a system to perform its specified function under permissible operating condition during a given time period, can be quantified using measures of reliability, availability, or time to failure. Safety, the absence of unacceptable risks, is a further measure of interest. Various methods for dependability evaluation exist, each with different variations and properties. In complex systems, more than one method is used. There is no one-for-all technique.

The best selection depends on the intended objective and other factors, e.g., the availability of tools, or the experience of the staff with a method. An operator may be interested in an estimate of the reliability of components to prepare a cost-effective maintenance plan. He could optimize stock size, availability, or down time. In terms of consequences or legislator requirements, his estimate doesn’t need to fulfill precise confidence limits. On the other side a safety authority might require the system supplier to provide definitive evidence with given confidence limits that the safety is within the tolerable bounds. The authorities are not interested in best estimates for safety. Instead they need resistant worst-case conservative evidence of the system hazardous failure rate being lower than the tolerable limit in order to grant their authorization.

Nevertheless, before the eventual authorization they need also evidence that as far as reasonably practicable all has been done to build a safe system.
Appropriate methods (including dependability evaluation methods) have to be applied all over the lifecycle of a system, from concept phase over design phases, to the eventual disposal phase of the system. Since the same techniques can be applied in different variations at different phases, a classification of methods is not directly obvious.

Here a classification is made by the intent of the method, whether it is used for forecasting or for verification of dependability. This leads to three classes of dependability evaluation methods that may provide useful dependability evidence (Table 1.2-1).

<table>
<thead>
<tr>
<th>Dependability Evaluation by</th>
<th>Analysis of process (e.g., residual fault density in similar projects) and product (e.g., analysis of credible failures of different levels of abstraction of the system)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Analysis</td>
<td>Evidence from observation (incident reports) for the used system from previous use in similar operational profiles</td>
</tr>
<tr>
<td>2. Field Experience</td>
<td>Providing representative inputs and testing for expected outputs for dependability testing equates to Fault Injection Testing (equipment failure testing)</td>
</tr>
<tr>
<td>3. Testing</td>
<td></td>
</tr>
</tbody>
</table>

It is noteworthy that field experience can be regarded as a specific kind of “long-term” testing. Testing and Field Experience are measurements of dependability properties, that providing direct evidence. Many practical fault injection campaigns that use an abstraction layer of the real system under evaluation are classified as “Analysis Methods” here. Specific methods and their applicability are discussed in the following sections.

2. DEPENDABILITY EVALUATION BY ANALYSIS

Analysis can be applied to various stages of the life cycle. The following considerations typically apply for safety evaluation, but similar applies to other dependability measures. In this case consequences of hazards include additional dependability categories (e.g., one train unavailable – minor delay ... all trains unavailable – complete loss of service).

Early in lifecycle, when only System Concept is available without realization details, typically some of the following measures are applied (without claim of completeness):

– Comparative Studies:
  Initial estimates based on experience from similar systems
– Preliminary Hazard Identification and Analysis PHIA: