Klintist Dyrmishi

Smart Style Software Engineering Project

Dependability Requirements

Dependability requirements are a large topic but I tried to narrow it down by doing some research.

There is a lot of information online according this topic so i picked the most repeated ones and tried to apply them to our business.

In system engineering, dependability is a measure of a system's availability, reliability, and its maintainability, and maintenance support performance, and, in some cases, other characteristics such as durability, safety and security.

Basically dependability is the ability to provide service/services that can be trusted by the user. They feel safe and protected while using the website.

Dependability can be broken down in three main elements: **Attributes, Threats, and Means**.

- Attributes: a way to assess the dependability of a system. Attributes are qualities of a system. These can be assessed to determine its overall dependability using Qualitative or Quantitative measures.
- Threats: Understandings of the things that can affect the dependability of a system. Threats are things that can affect a system and cause a drop in Dependability.
- Means: ways to increase a system's dependability.

There are further and more complex explanations of these main elements which I researched and I will include some of them.

Attributes:

- Availability - readiness for correct service
- Reliability - continuity of correct service
- Safety - absence of catastrophic consequences on the user(s) and the environment
- Integrity - absence of improper system alteration
- Maintainability - ability for easy maintenance (repair)

These are the definitions that define attribute from which Availability and Reliability are the only ones quantifiable by direct measurements, while the others are more subjective. Safety cannot be measured directly via metrics but is a subjective assessment that requires judgmental information to be applied to give a level of confidence, whilst Reliability can be measured as failures over time.

Threats:

There are three main terms that must be clearly understood:

- **Fault**: A fault (which is usually referred to as a bug for historic reasons) is a defect in a system. A fault in the system could or could not lead to a failure. Although a system may contain a fault, its input and state conditions may never cause this fault to be executed so the error doesn't occurs, which means that this particular fault does not exhibit as failure.

- **Error**: An error is a discrepancy between the intended behavior of a system and its actual behavior inside the system boundary. Errors occur at runtime when some part of the system enters an unexpected state due to the activation of a fault. Since errors are generated from invalid states they are hard to observe without special mechanisms, such as debuggers or debug output to logs.

- **Failure**: A failure is an instance in time when a system displays behavior that is contrary to its specification. An error may not necessarily cause a failure, for instance an exception may be thrown by a system but this may be caught and handled using fault tolerance techniques so the overall operation of the system will conform to the specification**.**

Means:

Since the mechanism of a **Fault-Error-Chain** is understood we can construct means to break the chains and increase the dependability of the system. Four means have been identified so far:

1. Prevention
2. Removal
3. Forecasting
4. Tolerance

- **Fault Prevention:** deals with prevention faults being incorporated into the system. This can be accomplished by development methodologies and good implementation techniques.

- **Fault Removal:** it can be divided into two sub-categories: **Removal during Development** and **Removal during Use.**

- **Removal:** during development verification is required so that faults can be found or detected and removed before the system is put in production. Once systems has been put in production

than we need another system to record failures and remove them via a maintenance cycle.

- **Fault Forecasting:** predicts likely faults so that they can be removed or their effects can be prevented.

We can use all of the above on our website in order to avoid any failure on the system or any corruption. Protection is one of the main points where we will focus and by getting a better knowledge on the faults, attributes, means and everything else we will be able to have a high maintenance of the system and guarantee the defense of the users where they will be protected. By being a step ahead of the faults we will avoid many of issues and errors.

Security requirements

Security requirements will include a wide area but the main requirements are:

1. Authentication and password management
2. Authorization and role management
3. Audit logging and analysis
4. Network and data security

Authentication and password are the some of the most important requirements that we will focus as mentioned before because security is the best way to gain trust. Authentication will always notify the user if something is wrong or not valid and according to the password we will try and make it invisible in the database like showing apteryx "*" instead of numbers and letters. This way the password will be protected all the time.

Authorization and role management will separate the users from employees and administrators where every account will have their limits with administrator being the main account which has access in the databases.

If you are recording any information at all, you are logging. Auditing, however, is more complex. Auditing is the practice of inspecting logs for the purpose of verifying that the system is in a desirable state or to answer questions about how the system arrived at a particular state. In this way we will be able to see where our website stands and how well it is doing.

Network and data security means that we need to protect our data and information from being infected or reached from a third party. This is a worldwide problem and customers get more and more aware of these issues and demand their privacy protected and defended which is one of the main points we will focus on our site.