EMSS 11

RELIABILITY AND AVAILABILITY REQUIREMENTS

Amol Shandilya, Yanyan Jiang, Minghui Jin

The Booch Group

1. Dependability Requirements

Requirement	Description	Plan
Error logs	User might input error log-in data or forget his account information, the system should correctly deal with this problem and let the user successfully log in to his account.	1. If the user input wrong information when logging in, then the system should ask him again for another input. When the user has tried for 5 times, then the system shall lock the account and the user shall only unlock the account by his email. 2. When the user forgets his account, the system shall allow the user to choose to log into the account by answering security questions, like what is the name of your first pet, whose answer has been stored when the user first created his account, and reset the code. Or the system shall allow the user to reset his account code by sending an email to his mailbox.
Response time	The response time of user input, each use cases and total system response time. When the user input command, the system should respond in 0.5ms. Each use case's runtime should within 2.5ms. The total responding time should within 1s.	The response time shall be collected when running the program. This could be achieved by configuring formal model code in each module of the program and the time shall be automatically calculated. Any component with runtime over 2.5ms shall be formal reviewed.
Clear messages	The system must send clear messages to the user without confusion.	The messages that send to the user is first defined by managers and developers, however whether they are really clear or not is defined by users. So, this one should be tested by user testing. Then, collect user feedback and make corresponding changes.

Fault tolerant	The system code must have backup for at least critical components. And error-prone code that would not impact the system shall be ignored.	1. Achieve backup. During programming, in terms of critical components, implement these components using various methods, and the original one together with the optimized one shall both be stored. Once the system fails, the original version or other method should go on working as the system backup. 2. Some of the use cases might the same functionality. As different use cases shall be implemented by different developer teams, the function might be implemented using different code. So, these methods could be cross-checked for their availability under different environment, and also shall be the backup of each other. Such as when planning the switch of power supply, device turn on/off, the two use cases can be implemented as switch function by two developer teams. 3. Using practices such as ensuring hardware redundancy, guarding against power loss, routinely installing security updates and antivirus measures, and monitoring server activity.

2. Measurement Requirements

Requirement	Plan	Where to use
POFOD	The POFOD shall be calculated when doing test. The testers or the users input one requests for hundreds of times, then change the environment and repeat above step. Then collecting the data and assess the probability that the system might fail corresponding to a request. Also, collect system response time and the impact of failure conditions.	1. Switch supply 2. Switch device status 3. Send notification 4. Sell excess 5. Read status of switches and source 6. Each program module’s input and respond (internal measure)

	The system failure includes system failure and system restart that would cause service interruptions. The POFOD shall be calculated not only for external command, but also the internal commands through the interfaces. And the internal measurement shall be implemented within the program.	
AVAIL	The AVAIL is used for continuously running system, taking repair and restart times into account. In terms of all monitoring system, using internal code to monitor the failure or error of the operational system.	1. The thermostat system 2. The device status monitoring system 3. The battery level monitoring system