4.2.2.2 Availability

Return to Reliability

About

return to the top

Availability in this context is System Availability. System Availability is the probability the system will function as designed for a particular duration. The duration could be a fixed time period (i.e., 24 hours a day, 7 days a week, or 364.9 days a year) or it could be over a particular mission (i.e., a flying mission, a patient stay, or a growing season). The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a time interval, assuming the required external resources are provided. [1)]

It is important to remember that Availability is expressed as a probability expressed in terms of Five Nines, and therefore, the Multiplication Rule of Probability needs to be considered when thinking about a system comprised of parts. Each part has its own probability of success (or failure). The **Multiplication Rule of Probability** means that to find the probability of the intersection of two events, multiply the two probabilities. The intersection of the events occurs when the probability of two events occurring is known. The Multiplication Rule of Probability determines the intersection of two different sets of events, called independent and dependent events.

- An Independent Event is when the probability of an event is not affected by a previous event.
- A Dependent Event is when one event influences the outcome of another event in a probability scenario. To find the intersection of two events, whether they are independent or dependent, multiply the two probabilities together. [2)]

Mission Duration (T_m) is the time the system needs to be operational. T_m can be expressed as a fixed time period (i.e., 24 hours a day, 7 days a week, or 365 days a year) or it could be over a particular mission (i.e., a flying mission, a patient stay, peak energy demand, or a growing season)

Mean Time Between Failure (MTBF) is a calculation of the arithmetic mean (average) time between failures of a system.

- **Note:** If a system is designed with both redundancy and automatic fault bypass, then MTBF is the anticipated lifespan of the system if these features cover all possible failure modes (infinity for all practical purposes). Such systems will continue without noticeable interruption when these conditions are satisfied unless there are secondary failures. This is called active redundancy and requires no maintenance to prevent mission failure. Active redundancy is required for systems that cannot be maintained, such as satellites. See: Wikipedia, Mean Time Between Failure (MTBF), Accessed 3 July 2020, https://en.wikipedia.org/wiki/Availability_(system)

- **Note:** The term is used for repairable systems[3)]

Downtime (T_d) is the Mission Duration times the sum of all of the different kinds of time required to transition from being down to the time to be fully operational, divided by the Mean Time Between Failure.

- Mean Time To Repair (MTTR) is the time required to restore operations the level defined in the system specification
- Mean Logistics Delay Time (MLDT) is the time required to obtain parts from the part depot or from the manufacturer including transportation to the site
- Mean Active Maintenance Down Time (MAMDT) is the average time required to perform diagnostics and replace parts

DDS Specifics

return to the top

Please refer to the **Note** in the MBTF section above.

Data Distribution Service (DDS) systems are generally architected, designed and implemented to provide redundancy and Failover in the event of a failure of Safety-Critical System (SCS) and Mission Critical Systems.

DDS allows for multiple Publishers and Subscribers of data to the same Topic at the same time. The Quality of Service (QoS) Policies parameters set by each publisher and each subscriber are used to connect them together.

For example, if the temperature in a chemical mixing tank is critical to the overall process, having multiple temperature sensors in the mixing tank at the same time allows for redundancy for the critical Sensor. If one of the two sensors fail, the DDS Middleware will automatically start routing the data published by the backup sensor to the subscribers.

Similarly, if the monitor listening to the Topic is considered critical to the chemical mixing process, the system can use redundant monitors. The monitors watch the data on the Topic and make adjustments to the the system to correct temperature variations thereby keeping the temperature in the correct operating range. The monitor does this by publishing information on a different Topic monitored by Actuators while making the appropriate adjustments.

1)
Note: Availability is part of Reliability, Maintainability, and Availability (RAM)

2)
The Multiplication Rule of Probability: Definition & Examples, Chapter 4, lesson 11, Accessed 3 July 2020, https://study.com/academy/lesson/the-multiplication-rule-of-probability-definition-examples-quiz.html

3)
https://en.wikipedia.org/wiki/Mean_time_between_failures | Mean Time Between Failure (MTBF)]]

From:
https://www.omgwiki.org/dido/ - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.4_req:2_nonfunc:14_reliability:02_availability&rev=1605745656

Last update: **2020/11/18 19:27**