Measuring System Availability

How Telecom & IT industries manage the impact of software reliability

January 9, 2017

Impact of SW faults is difficult to classify

Fault vs. Failure is determined in the context of the system

- Example: Software directed reset of circuit card
  In redundant architecture, system heals without any loss of function…

- Depending on the system architecture, a SW fault may yield:
  No Impact,
  Reduced capability, or
  Loss of function

- Metrics relevant under one architecture are irrelevant under another. How do we choose what to focus on?

What do we actually want to improve?

System availability

- Loss of system function (uptime, system failure)

- Quality of system function (performance, bandwidth)

Software

- Software Faults (exceptions, log events, unexpected state)

Software faults are not the problem…only the subset that result in system failures

Measure the problem (System Availability) to drive improvement

Methods from other industries:

Telecom

- Service Level Agreements (SLAs) formalize:

  - Guarantees of availability* (bandwidth, traffic shaping, quality of service, etc.)

  - Support guarantees (reaction time, notification, etc.)

  - Measures of compliance*

  - Penalties for non-compliance

Information Technology

- Service Level Agreements (SLAs) formalize:

  - Guarantees of availability* (uptime, latency, performance, etc.)

  - Response/Support expectations

  - Measures of compliance*

  - Penalties for non-compliance

  - Compliance to SLAs demonstrated through external monitoring and self-reporting

Enforcing System Availability

Advantages from Telecom & IT

- Contracts are independent of the system architecture
  Only the system failures that matter are measured

- Vendors are free to innovate fault-tolerance
  Software metrics are not coupled to the contractual approach

- Customers have recourse for poor reliability
  Regardless of cause (SW, HW, or System)

Considerations for SLAs in Avionics

- External monitoring (adding dedicated monitoring systems/functions) may be difficult to add

- Self-reporting can be ambiguous without external system support

- Regulatory requirements (certification) complicate support guarantees

- SLAs are typically funded through ongoing support fees paid by customer, with penalties for non-compliances.

- SLAs depend upon data sharing. Vendors would likely need to get full-flight log data from covered systems to monitor/improve reliability.