Fault-Hypothesis of IEEE 802.1Q AVB and Redundancy Management

IEEE Interim Meeting, Santa Cruz, Sep/2012

Wilfried Steiner, Senior Research Engineer
wilfried.steiner@tttech.com

What is a Fault Hypothesis ?

A Fault-Hypothesis (FH) defines things like*:

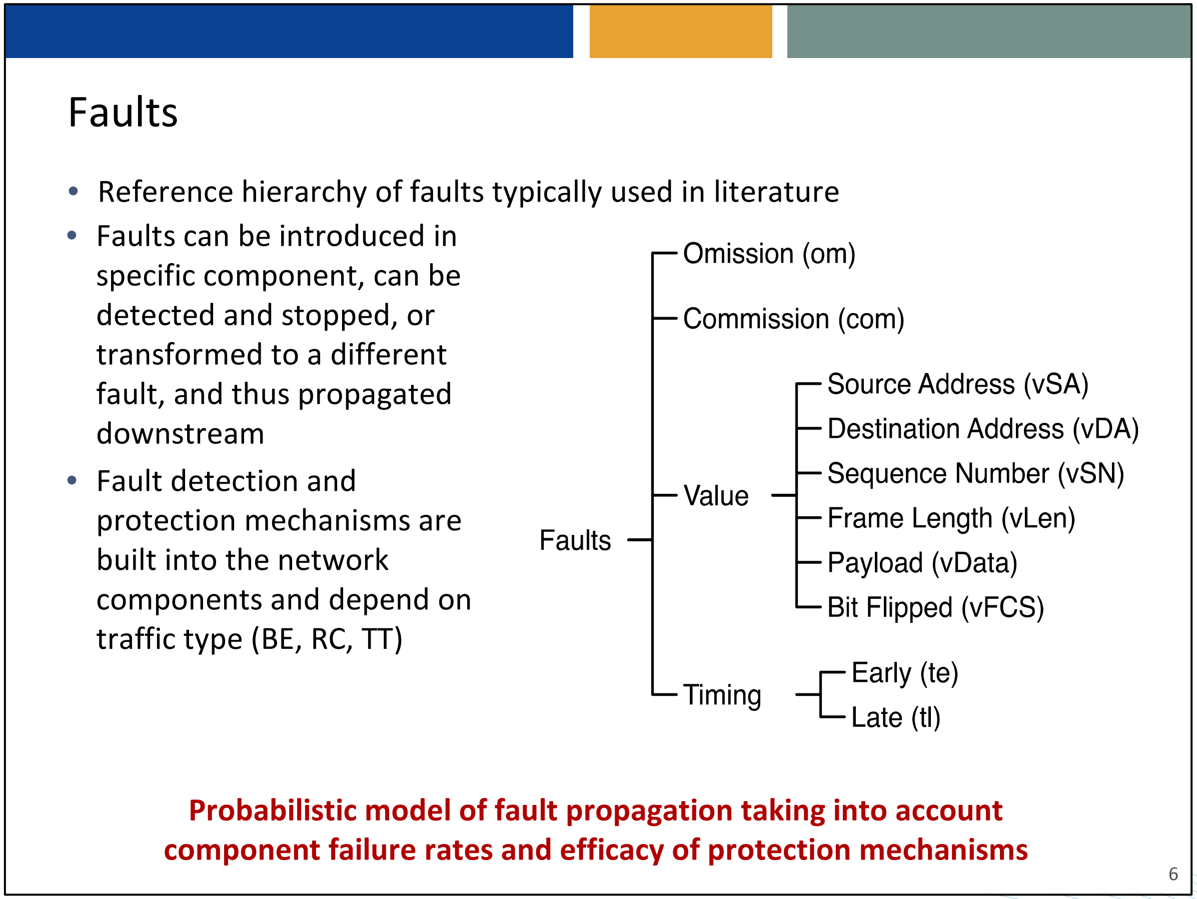
- Fault-Containment Region
  - Where are the boundaries of the physical entity affected by a fault?
- Failure Mode
  - May we consider simple failures only (e.g., a faulty component will be silent), or do we need to expect malicious failure behavior?
- Failure Frequency
  - How often may failures occur?
- Error Detection Latency
  - How long does it take to detect a failure?
- Recovery Intervals
  - How long does it take to recover from a failure?

In critical systems, these may be autonomous actions without human interaction.

→ Essentially, the FH is another set of assumptions.

*Kopetz, H., „*On the Fault Hypothesis for a Safety-Critical Real-Time System*,“ In Proceedings of the Automotiove Workshop, 2004, p. 14-23

Example of possible Failure Modes in an Ethernet Network



Faults

- Reference hierarchy of faults typically used in literature
- Faults can be introduced in specific component, can be detected and stopped, or transformed to a different fault, and thus propagated downstream
- Fault detection and protection mechanisms are built into the network components and depend on traffic type (BE, RC, TT)

Faults
- Omission (om)
- Commission (com)
- Value
  - Source Address (vSA)
  - Destination Address (vDA)
  - Sequence Number (vSN)
  - Frame Length (vLen)
  - Payload (vData)
  - Bit Flipped (vFCS)
- Timing
  - Early (te)
  - Late (tl)

Probabilistic model of fault propagation taking into account component failure rates and efficacy of protection mechanisms

6

*From Briesemeister et.al., „*Quantitative Fault Propagation Analysis for Networked Cyber-Physical Systems*,“ 2011, Available from http://www.csl.sri.com/papers/AVICPS2011/

Why is the Fault Hypothesis relevant for Redundancy Management?

Redundancy Management (RM) *is a means* to increase dependability and reliability of a system *to tolerate failures*.

Hence, RM and FH are strictly related to each other, which gives the following two options:

- Option 1: Define RM first and then calculate which failures are tolerated (i.e., the FH).
- Option 2: Define FH first and then design RM.

The straight-forward way is Option 2 (that’s how we typically solve engineering problems).

However, as we strive for generality of applicability of the RM solution, cyclically alternating between Option 1 and Option 2 is likely to be necessary.

Nevertheless, I think that in this process of (re-)defining the RM we also need to explicitly define a FH (which may be updated as we refine the RM).

→ And a proposal of an FH for IEEE 802.1Q AVB may be as follows.

Proposal – IEEE 802.1Q AVB Failure Hypothesis

Fault-Containment Regions (FCR):

- Communication Link
- End Station
- Bridge

→ A fault is local to either an end station or a bridge or a communication link.

→ If more than one bridge / one end stations / one link become faulty then we have also more than one fault.

Failure Mode for End Stations and Bridges

- Permanent, Consistent, and Fail-Silent

→ In the case of a failure, a faulty FCR will stop producing output (“Fail-Silent”).

→ A faulty FCR will behave the same on all ports, e.g., a faulty bridge will stop producing output on all ports (“Consistent”).

→ A faulty FCR will be faulty for the remaining mission time (“Permanent”).

Failure Mode for Communication Links

- Transient or Permanent, Detectably Faulty

→ The communication link may drop frames or invalidate the Ethernet FCS on a per frame basis (“Transient”).

→ The communication link may become unavailable for the remaining mission time (“Permanent”).

→ Each failure of the communication link results in either a loss of the frame or an invalidation of the frame’s FCS (“Detectably Faulty “).

Example Redundancy Management Service that satisfies the Fault Hypothesis: ARINC 664-p7

ARINC 664-p7 is an avionics standard for using Ethernet in an airplane.

In simple terms it operates as follows:

ARINC 664-p7 uses sequence numbers to identify matching copies of redundantly transmitted frames.

The transmitting end station is connected to two networks and sends the same frame with the same sequence numbers on both networks.

The redundancy management at the receiving end station is split into two subroutines:

1. "Integrity Checking"
2. "Redundancy Management" (to avoid confusion I call this subroutine RM-A664)

Integrity checking is used to identify whether the sequence number in a received frame is "plausible" i.e., within a configurable window (e.g., +1 or +2) higher than the sequence number in the previously received frame

RM-A664 forwards the first received copy of a frame to the host which matches the integrity check and throws away all other copies with the same sequence number for a configured time (started at the reception of the first frame).

TTTech

Ensuring Reliable Networks

www.tttech.com