Fault detection and Fault tolerance with TSF and MVTISA in P802.1ASed Draft 2.0

Abdul Jabbar, GE Aerospace Research

Richard Tse, Microchip

Why not use simple midpoint selection like fault-tolerant midpoint

- FTM is specified in 8.6 of the FlexRay Communications System Protocol Specification (v2.1):
  - https://www.plus.ac.at/wp-content/uploads/2021/02/FlexRayCommunicationSystem.pdf
  - FlexRay is used in automotive systems and FTM is used in its clock synchronization mechanism.
  - FTM algorithm:
    - Input data is sorted by their values, from smallest to largest
    - The K largest and K smallest data values are discarded, where
      - K = 0 if there are 1 or 2 input data values
      - K = 1 if there are 3 to 7 input data values
      - K = 2 if there is > 7 input data values
    - The output of the FTM is the average of the remaining largest and smallest data values

- The FTTM, with MVTISA, also considers the removal of values from a set of data before selecting the middle value:
  - The number of values to be removed and the selection of each value that is removed is based on whether the value is trusted (i.e., matches expectations relative to the other values) rather than just being an extremity
  - The middle value from the trusted values is selected (averaging is not used as this would create a new gPTP domain)

FTM vs FTTM – detectability of faults

Case 1: independent times with uncorrelated faults

FTTM: 13:20, 14:20, 15:20, 10:20 → NQ

FTM: 10:20 13:20, 14:20, 15:20, → 13:50

Case 2: dependent times with correlated faults

FTTM: {13:20, 13:22, 13:25}, 10:20 → 13:22, 10:20 → NQ (with DTSF)

FTM: {13:20, 13:22, 13:25}, 10:20 → 13:22, 10:20 → 11:51 (with DTSF)

FTM: 13:20, 13:22, 13:25, 10:20 → 13:21 (without DTSF)

Case 3: independent times with correlated faults

FTTM: 08:20, 08:24, 10:18, 10:20 → either 8:24 or 10:18

FTM: 08:20, 08:24, 10:18, 10:20 → 9:21

Summary:

FTM's averaging creates a new gPTP domain, which is not desired

FTM cannot give NQ as result.

There are many fault cases where NQ is the desired result…. and this detectability is not supported by FTM

Both FTTM and FTM are not fault tolerant for cases where independent times have correlated faults AND number of times is less than (2n+1) for n faults

FTM vs FTTM – tolerance/survivability for independent times with uncorrelated faults

CASE 4: 3 faulty and 2 non-faulty times

FTTM: 13:20, 14:20, 15:20, 10:20, 10:25: → 10:20, 10:25 → 10:20

FTM:, 10:20, 10:25, 13:20, 14:20, 15:20, → 12:22.5

CASE 5: 2 faulty and 2 non-faulty times

FTTM: 13:20, 14:20, 10:20, 10:25: → 10:20, 10:25 → 10:20

FTM:, 10:20, 10:25, 13:20, 14:20, → 11:52.5

CASE 6: 1 faulty and 2 non faulty times

FTTM: 13:20,, 10:20, 10:25: → 10:20, 10:25 → 10:20

FTM:, 10:20, 10:25, 13:20, → 10:25

Summary:

FTM (aside from the undesired averaging) is unlikely to produce a correct result if all faulty inputs are not discarded as any remaining faulty input is likely to be an extremity and will be used in the averaging.

FTTM will select correct time if there are at least 2 non-faulty inputs and the faulty inputs are not correlated (i.e., do not mimic a trusted pair).

FTM vs FTTM – tolerate/survive for dependent times with correlated faults

CASE 7: dependent times + independent

FTTM: {13:20, 13:25, 13:22}, 10:20, 10:25 → 13:22, 10:20, 10:25 → 10:20

FTM: 10:20, 10:25, {13:20, 13:22, 13:25} → 13:22, 10:25, 10:20, → 10:25

CASE 8: dependent + more independent

FTTM: {13:20, 13:25, 13:22}, 10:22, 10:25, 10:18, 10:20 → 13:22, 10:20, 10:25, 10:18, 10:22 → 10:20

FTM: 10:20, 10:25, 10:18, 10:22, {13:20, 13:25, 13:22} → 13:22, 10:25, 10:22, 10:20, 10:18 → 10:22.5*

Summary:

For these dependent faults, FTTM and FTM (*aside from its averaging) both produce valid results.

FTM discards faulty inputs in these examples.

Comparison

Input Times	Fault Correlation	FTTM (2 stage) with MVTISA		Fault Tolerant Midpoint (one stage or two stage) FLEX RAY	
		Fault Detection	Fault Survivability	Fault Detection	Fault Survivability
Independent Times	Uncorrelated faults	Yes, for all cases	Yes, if there is a single pair of correct input times	Not available	Only if faulty inputs are at large and small extremes and are discarded
Dependent Times	Correlated Faults	Yes, for all cases (with ITSF)	Yes, if there are (2n+1) inputs for n faults	Not available	Only if faulty inputs are discarded
Independent Times	Correlated Faults	Yes, if there are (2n+1) inputs for n faults	Yes, if there are (2n+1) inputs for n faults	Not available	Unlikely, a faulty input is likely to remain (i.e., not discarded) and be used in the averaging

Comparison

Input Times	Fault Correlation	FTTM (2 stage) with MVTISA		General Fault Tolerant Midpoint (one stage or two stage)	
		Fault Detection	Fault Survivability	Fault Detection	Fault Survivability
Independent Times	Uncorrelated faults	Yes, for all cases	Yes, if there is a single pair of correct input times	Not available	Only if faulty inputs are at large and small extremes and are discarded
Dependent Times	Correlated Faults	Yes, for all cases (with ITSF)	Yes, if there are (2n+1) inputs for n faults	Not available	Only if faulty inputs are discarded
Independent Times	Correlated Faults	Yes, if there are (2n+1) inputs for n faults	Yes, if there are (2n+1) inputs for n faults	Yes, if there are (2n+1) inputs for n faults	Yes, if there are (2n+1) inputs for n faults