Appendix

Proposition and theorem proofs

This appendix contains the proofs for Propositions 1-2 and Theorem 2.

Proposition 1:

Proof. Let $G_{t\Delta F}$ be the TDES constructed in Algorithm 1

Let $G_{\Delta F}$ be the DES constructed in Algorithm 1 in Mulahuwaish.[3]

We note that the two are identical except that $G_{t\Delta F}$ adds *tick* to its event set, and *tick* is selflooped at every state.

Let $G' = G \| G_{t\Delta F}$ as per Algorithm 3.

Let $G'' = G \| G_{\Delta F}$ as per Algorithm 3 in Mulahuwaish.[1]

As the event set of G already contains *tick*, and *tick* is selflooped at every state of $G_{t\Delta F}$, it follows that $L(G') = L(G'')$

The result then follows from Proposition 1 of Mulahuwaish[1] which states:

$\left(\forall s \in L(G) s \notin L_{\Delta F} \Leftarrow s \in L(G")\right)$.

Proposition 2:

Proof. Let $G_{t\Delta F}$ and $G_{t1RF_1}, \ldots, G_{t1RF_m}$ be the TDES constructed in Algorithms 1 and 2.

Let $G_{\Delta F}$ and $G_{1RF_1}, \ldots, G_{1RF_m}$ be the DES constructed from Algorithms 1 and 2 in Mulahuwaish.[2]

We note that each pair is identical except that $G_{t\Delta F}$ and $G_{t1RF_1}, \ldots, G_{t1RF_m}$ add *tick* to their event sets, and *tick* is selflooped at every state.

Let $G' = G \| G_{t\Delta F} \| G_{t1RF_1} \| \ldots \| G_{t1RF_m}$ as per Algorithm 4.

Let $G" = G \| G_{\Delta F} \| G_{1RF_1} \| \ldots \| G_{1RF_m}$ as per Algorithm 5 in Mulahuwaish.[2]

As the event set of G already contains *tick* , and *tick* is selflooped at every state of $G_{t\Delta F}$ and $G_{t1RF_1}, \ldots, G_{t1RF_m}$, it follows that $L(G') = L(G'')$.

The result then follows from Proposition 2 of Mulahuwaish,[2] which states:

$\left(\forall s \in L(G)(s \notin L_{\Delta F}) \wedge \left(s \in L_{1RF_m}\right) \Leftarrow s \in L(G")\right)$

Theorem 2

Proof. Assume initial conditions for the theorem.

We first note that if $m = 0$, we have $\Sigma_F = \varnothing$ and the proof is identical to the proof of Theorem 1. We can thus assume $m \geq 1$ for the rest of the proof without any loss of generality.

Must show S is timed m-one-repeatable fault-tolerant controllable for $G \Leftrightarrow S$ is controllable for G'.

From Algorithm 4 we have $G' = G \| G_{t\Delta F} \| G_{t1RF,1} \| \ldots \| G_{t1RF,m}$.

From Algorithm 1, we know that $G_{t\Delta F}$ is defined over $\Sigma_{\Delta F} \cup \{\tau\}$, and from Algorithm 2, we know that $G_{t1RF,m}$ is defined over $\Sigma_{F_i} \cup \{\tau\}$, $i = 1, \ldots, m$.

Let $P_{t\Delta F} : \Sigma^* \to (\Sigma_{\Delta F} \cup \{\tau\})^*$, and $P_{tF_i} : \Sigma^* \to (\Sigma_{F_i} \cup \{\tau\})^*$, $i = 1, \ldots, m$, be natural projections.

As G is defined over Σ, we have that $L(G') = L(G) \cap P_{t\Delta F}^{-1} L(G_{t\Delta F}) \cap P_{tF_1}^{-1} L(G_{t1RF,1}) \cap \ldots \cap P_{tF_m}^{-1} L(G_{t1RF,m})$.
(T4.1)

Part A Show (⇒).

Assume S is timed m-one-repeatable fault-tolerant controllable for G. (T4.2)

Must show implies: $(\forall s \in L(S) \cap L(G'))$

$$Elig_{L(S)}(s) \supseteq \begin{cases} Elig_{L(G')}(s) \cap (\Sigma_u \cup \{\tau\}) & if \ Elig_{L(S) \cap L(G')}(s) \cap \Sigma_{for} = \varnothing \\ Elig_{L(G')}(s) \cap \Sigma_u & if \ Elig_{L(S) \cap L(G')}(s) \cap \Sigma_{for} \neq \varnothing \end{cases}$$

Let $s \in L(S) \cap L(G')$. (T4.3)

We have two cases: (A.1) $Elig_{L(S)\cap L(G')}(s)\cap\Sigma_{for}=\varnothing$, and (A.2) $Elig_{L(S)\cap L(G')}(s)\cap\Sigma_{for}\neq\varnothing$.

Case A.1 $Elig_{L(S)\cap L(G')}(s)\cap\Sigma_{for}=\varnothing$

Let $\sigma\in\Sigma_u\cup\{\tau\}$. Assume $s\sigma\in L(G')$. (T4.4)

Must show implies $s\sigma\in L(S)$.

To apply (T4.2), we need to show that $s\in L(S)\cap L(G)$, $s\sigma\in L(G)$, $s\notin L_{\Delta F}$, and $s\in L_{1RF_m}$, and $Elig_{L(S)\cap L(G)}(s)\cap\Sigma_{for}=\varnothing$.

We first note that (T4.1), (T4.3) and (T4.4) imply:
$s\in L(S)$, $s\in L(G)$, and $s\sigma\in L(G)$

As $s\in L(G')$ by (T4.3), we conclude by Proposition 2 that: $s\notin L_{\Delta F}$, and $s\in L_{1RF_m}$.

We will now show that $Elig_{L(S)\cap L(G)}(s)\cap\Sigma_{for}=\varnothing$.

It is sufficient to show:
$(\forall\sigma'\in\Sigma_{for})s\sigma'\notin L(S)\cap L(G)$

Let $\sigma'\in\Sigma_{for}$. Must show implies $s\sigma'\notin L(S)\cap L(G)$.

We note that, by assumption, $Elig_{L(S)\cap L(G')}(s)\cap\Sigma_{for}=\varnothing$.

This implies: $(\forall\sigma''\in\Sigma_{for})s\sigma''\notin L(S)\cap L(G')$

It thus follows that $s\sigma'\notin L(S)\cap L(G')$.

$\Rightarrow s\sigma'\notin L(S)\cap L(G)\cap P_{t\Delta F}^{-1}L(G_{t\Delta F})\cap P_{tF_1}^{-1}L(G_{t1RF,1})\cap\ldots\cap P_{tF_m}^{-1}L(G_{t1RF,m})$, by (T4.1)

To show $s\sigma'\notin L(S)\cap L(G)$, it is sufficient to show $s\sigma'\in P_{t\Delta F}^{-1}L(G_{t\Delta F})\cap P_{tF_1}^{-1}L(G_{t1RF,1})\cap\ldots\cap P_{tF_m}^{-1}L(G_{t1RF,m})$.

As S and G are timed fault-tolerant consistent and $\Sigma_{for}\subseteq\Sigma_{act}$, it follows that $\Sigma_{for}\cap(\Sigma_{\Delta F}\cup\Sigma_F\cup\{\tau\})=\varnothing$

$\Rightarrow P_{t\Delta F}(s\sigma')=P_{t\Delta F}(s)P_{t\Delta F}(\sigma')=P_{t\Delta F}(s)$

Similarly, we have $P_{tF_i}(s\sigma')=P_{tF_i}(s)$, $i=1,\ldots,m$.

As $s\in L(G')$ by (T4.3), we have $s\in P_{t\Delta F}^{-1}L(G_{t\Delta F})\cap P_{tF_1}^{-1}L(G_{t1RF,1})\cap\ldots\cap P_{tF_m}^{-1}L(G_{t1RF,m})$ by (T4.1).

$\Rightarrow P_{t\Delta F}(s)\in L(G_{t\Delta F})$, and $P_{tF_i}(s)\in L(G_{t1RF,m})$, $i=1,\ldots,m$

$\Rightarrow P_{t\Delta F}(s\sigma')\in L(G_{t\Delta F})$, and $P_{tF_i}(s\sigma')\in L(G_{t1RF,m})$, $i=1,\ldots,m$

$\Rightarrow s\sigma'\in P_{t\Delta F}^{-1}L(G_{t\Delta F})\cap P_{tF_1}^{-1}L(G_{t1RF,1})\cap\ldots\cap P_{tF_m}^{-1}L(G_{t1RF,m})$

We thus conclude that $Elig_{L(S)\cap L(G)}(s)\cap\Sigma_{for}=\varnothing$.

We can now conclude by (T4.2) that $s\sigma\in L(S)$, as required.

Case A.2 $Elig_{L(S)\cap L(G')}(s)\cap\Sigma_{for}\neq\varnothing$

Let $\sigma\in\Sigma_u$. Assume $s\sigma\in L(G')$.

Must show implies $s\sigma\in L(S)$.

Proof is identical to proof of Case (A.1) except without the need to show $Elig_{L(S)\cap L(G)}(s)\cap\Sigma_{for}=\varnothing$.

Part B Show $(\Leftarrow)$.

Assume S is controllable for G'. (T4.5)

Must show implies S and G are timed fault-tolerant consistent (follows automatically from initial assumptions) and that:

$$(\forall s\in L(S)\cap L(G))s\notin L_{\Delta F}\wedge s\in L_{1RF_m}\Rightarrow$$
$$Elig_{L(S)}(s)\supseteq\begin{cases}Elig_{L(G)}(s)\cap(\Sigma_u\cup\{\tau\}) & if\ Elig_{L(S)\cap L(G)}(s)\cap\Sigma_{for}=\varnothing\\ Elig_{L(G)}(s)\cap\Sigma_u & if\ Elig_{L(S)\cap L(G)}(s)\cap\Sigma_{for}\neq\varnothing\end{cases}$$

Let $s \in L(S) \cap L(G)$. (T4.6)

We have two cases: (B.1) $Elig_{L(S)\cap L(G)}(s) \cap \Sigma_{for} = \varnothing$, and (B.2) $Elig_{L(S)\cap L(G)}(s) \cap \Sigma_{for} \neq \varnothing$.

Case B.1 $Elig_{L(S)\cap L(G)}(s) \cap \Sigma_{for} = \varnothing$

Let $\sigma \in \Sigma_u \cup \{\tau\}$. Assume $s\sigma \in L(G)$ and $s \notin L_{\Delta F} \wedge s \in L_{1RF_m}$. (T4.7)

Must show implies $s\sigma \in L(S)$.

We have two cases: (B 1.1) $\sigma \in \Sigma_{\Delta F} \cup \Sigma_F$, and (B 1.2) $\sigma \notin \Sigma_{\Delta F} \cup \Sigma_F$.

Case B 1.1) $\sigma \in \Sigma_{\Delta F} \cup \Sigma_F$

As the system is timed fault-tolerant consistent, it follows that σ is self-looped at every state in S.

As $s \in L(S)$ by (T4.6), it thus follows that $s\sigma \in L(S)$, as required.

Case B 1.2 $\sigma \notin \Sigma_{\Delta F} \cup \Sigma_F$

To apply (T4.5), we need to show $s \in L(S) \cap L(G')$, $s\sigma \in L(G')$, and $Elig_{L(S)\cap L(G')}(s) \cap \Sigma_{for} = \varnothing$.

By (T4.6), (T4.7) and Proposition 2, we conclude: $s \in L(G')$ (T4.8)

We will next show that $s\sigma \in L(G')$.

As $s \in L(G')$, we have by (T4.1) that $s \in P_{t\Delta F}^{-1} L(G_{\Delta F}) \cap P_{tF_1}^{-1} L(G_{t1RF,1}) \cap \ldots \cap P_{tF_m}^{-1} L(G_{t1RF,m})$.

It thus follows that $P_{t\Delta F}(s) \in L(G_{t\Delta F})$, and $P_{tF_i}(s) \in L(G_{t1RF,m})$, $i = 1,\ldots,m$. (T4.9)

We have two cases: (B 1.2.1) $\sigma \neq \tau$, and (B 1.2.2) $\sigma = \tau$.

Case B 1.2.1 $\sigma \neq \tau$

As $\sigma \notin \Sigma_{\Delta F} \cup \Sigma_F \cup \{\tau\}$, we have $P_{t\Delta F}(\sigma) = \epsilon$.

$\Rightarrow P_{t\Delta F}(s\sigma) = P_{t\Delta F}(s) P_{t\Delta F}(\sigma) = P_{t\Delta F}(s)$

Similarly, we have $P_{tF_i}(s\sigma) = P_{tF_i}(s)$, $i = 1,\ldots,m$.

$\Rightarrow P_{t\Delta F}(s\sigma) \in L(G_{t\Delta F})$, and $P_{tF_i}(s\sigma) \in L(G_{t1RF,m})$, $i = 1,\ldots,m$, by (T4.9)

$\Rightarrow s\sigma \in P_{t\Delta F}^{-1} L(G_{t\Delta F}) \cap P_{tF_1}^{-1} L(G_{t1RF,1}) \cap \ldots \cap P_{tF_m}^{-1} L(G_{t1RF,m})$

Case B 1.2.2 $\sigma = \tau$

By Algorithms 1, and 2, we know that τ is selflooped at every state in $G_{t\Delta F}$, and $G_{t1RF,m}$, $i = 1,\ldots,m$.

$\Rightarrow P_{t\Delta F}(s)\sigma \in L(G_{t\Delta F})$, and $P_{tF_i}(s)\sigma \in L(G_{t1RF,m})$, $i = 1,\ldots,m$, by (T4.9)

$\Rightarrow P_{t\Delta F}(s\sigma) \in L(G_{t\Delta F})$, and $P_{tF_i}(s\sigma) \in L(G_{t1RF,m})$, by definitions of $P_{t\Delta F}$, and P_{tF_i}, $i = 1,\ldots,m$

$\Rightarrow s\sigma \in P_{t\Delta F}^{-1} L(G_{t\Delta F}) \cap P_{tF_1}^{-1} L(G_{t1RF,1}) \cap \ldots \cap P_{tF_m}^{-1} L(G_{t1RF,m})$

By Cases (B 1.2.1) and (B 1.2.2), we can conclude that $s\sigma \in P_{t\Delta F}^{-1} L(G_{t\Delta F}) \cap P_{tF_1}^{-1} L(G_{t1RF,1}) \cap \ldots \cap P_{tF_m}^{-1} L(G_{t1RF,m})$.

Combining with (T4.1) and (T4.7), we have $s\sigma \in L(G')$. (T4.10)

We will now show $Elig_{L(S)\cap L(G')}(s) \cap \Sigma_{for} = \varnothing$.

It is sufficient to show: $(\forall \sigma' \in \Sigma_{for}) s\sigma' \notin L(S) \cap L(G')$

Let $\sigma' \in \Sigma_{for}$. We will now show this implies $s\sigma' \notin L(S) \cap L(G')$.

We note that by assumption, we have $Elig_{L(S)\cap L(G)}(s) \cap \Sigma_{for} = \varnothing$.

$\Rightarrow (\forall \sigma'' \in \Sigma_{for}) s\sigma'' \notin L(S) \cap L(G)$

$\Rightarrow s\sigma' \notin L(S) \cap L(G)$

This implies $s\sigma' \notin L(S) \cap L(G) \cap P_{t\Delta F}^{-1} L(G_{t\Delta F}) \cap P_{tF_1}^{-1} L(G_{t1RF,1}) \cap \ldots \cap P_{tF_m}^{-1} L(G_{t1RF,m})$ as

$L(S)\cap L(G)\cap P_{t\Delta F}^{-1}L(G_{t\Delta F})\cap P_{tF_1}^{-1}L(G_{t1RF,1})\cap\ldots\cap P_{tF_m}^{-1}L(G_{t1RF,m}))\subseteq L(S)\cap L(G)$.

$\Rightarrow s\sigma'\notin L(S)\cap L(G')$, by (T4.1)

We thus conclude $Elig_{L(S)\cap L(G')}(s)\cap\Sigma_{for}=\varnothing$.

Combining with (T4.6), (T4.8), and (T4.10), we have:
$s\in L(S)\cap L(G')$, $s\sigma\in L(G')$, and $Elig_{L(S)\cap L(G')}(s)\cap\Sigma_{for}=\varnothing$.

We can now conclude by (T4.5) that $s\sigma\in L(S)$, as required.

We thus conclude by Cases (B 1.1) and (B 1.2) that $s\sigma\in L(S)$.

Case B.2 $Elig_{L(S)\cap L(G)}(s)\cap\Sigma_{for}\neq\varnothing$

Let $\sigma\in\Sigma_u$. Assume $s\sigma\in L(G)$ and $s\notin L_{\Delta F}\wedge s\in L_{1RF_m}$.

Must show implies $s\sigma\in L(S)$.

Proof is identical to proof of Case (B.1) except without the need to show $Elig_{L(S)\cap L(G')}(s)\ \cap\Sigma_{for}=\varnothing$.

We now conclude by Parts (A) and (B) that S is timed m-one-repeatable fault-tolerant controllable for G iff S is controllable for G'.