1 Proofs of Propositions

Proposition 1 *(Enforceability using the serial composition of EMs of a set of safety TAs satisfying syntactic conditions given in Def. 4.5). Consider n safety timed properties $\{\varphi_1, \varphi_2, \cdots, \varphi_n\}$ to be enforced. If their TAs satisfies the syntactic conditions (a) or (b) from Def.4.5 then, the given set of safety timed properties are enforceable using the serial composition approach (i.e., $E_{\varphi_1} \Rrightarrow E_{\varphi_2} \Rrightarrow \cdots \Rrightarrow E_{\varphi_n}$ is sound, transparent and satisfies the other constraints according to Def. 3.5 and Remark 2 and thus, is an EM for $\varphi_1 \cap \varphi_2 \cap \cdots \cap \varphi_n$).*

Proof of Proposition 1 . Proposition 1, talks about enforceability using the serial composition of a set of safety TAs satisfying syntactic conditions given in Def. 4.5. It says, consider n safety timed properties $\{\varphi_1, \varphi_2, \cdots, \varphi_n\}$ to be enforced. If their safety TAs satisfies the syntactic conditions (a) or (b) from Def. 4.5 then, the given set of safety timed properties are enforceable using the serial composition approach (i.e., $E_{\varphi_1} \Rrightarrow E_{\varphi_2} \Rrightarrow \cdots \Rrightarrow E_{\varphi_n}$ is sound, transparent and satisfies the other constraints according to Def. 3.5 and Remark 2; and thus is an EM for $\varphi_1 \cap \varphi_2 \cap \cdots \cap \varphi_n$.

Proof: Let there be two properties φ_i and φ_j (the proof will generalize to any number of properties) and let their enforcers be connected in series as $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$. Let at time t, input given to the system be σ where input processed by E_{φ_i} be $\sigma_i (= \sigma)$ and input processed by E_{φ_j} be σ_j. Let at time t, σ_{Ci} and σ_{Si} respectively be the buffer content and output released by E_{φ_i}. Similarly, σ_{Cj} and σ_{Sj}. Let at time $t' (= t + \delta)$, an action a arrives, thus input event is (δ, a).

Induction basis:
If $\sigma = \epsilon$ at time $t^0 (t^0 < t)$,
$E_{\varphi_i}(\epsilon, t^0) = \epsilon$ (from Def. 3.6)
which is given to E_{φ_j} at time t^0
$E_{\varphi_j}(\epsilon, t^0) = \epsilon$ (from Def. 3.6)
Hence, Proposition 1 trivially holds for $\sigma = \epsilon$.

Induction step:
Assume that the proposition holds at time t when input is σ.
Now, let us prove that the proposition holds for $\sigma \cdot (\delta, a)$ at time t'.

Considering syntactic condition (a) of Def. 4.5

Case 1: $K \neq \emptyset$ of E_{φ_i} (meaning we are able to find a timed word, by appropriately delaying $\sigma_{Ci} \cdot (\delta, a)$ by δ' s.t. φ_i is satisfied)
where $(v + \delta + \delta') \models g_i$ and $l'_i \in F$
σ_{Ci} would necessarily be empty (i.e., $\sigma_{Ci} = \epsilon$), since φ_i is a safety property.
Hence, $E_{\varphi_i}(\sigma_i, t') = \sigma_{Si} \cdot (\delta + \delta', a)$ (from Def. 3.6)

- $E_{\varphi_i}(\sigma_i, t) = \sigma_{Si}$ and $E_{\varphi_i}(\sigma_i, t') = \sigma_{Si} \cdot (\delta + \delta', a)$ and $t' \geq t$. Thus, **(Phy1)** is satisfied.
- $E_{\varphi_i}(\sigma_i, t') = \text{obs}\Big(\Pi_1\big(\text{store}_{\varphi_i}(\text{obs}(\sigma_i, t'))\big), t'\Big)$ and from definition and property of obs that $\forall \sigma : \text{time}(\text{obs}(\sigma_i, t')) \leq t$, applied to $\Pi_1\big(\text{store}_{\varphi_i}(\text{obs}(\sigma_i, t'))\big)$, we can conclude that $\text{time}(E_{\varphi_i}(\sigma_i, t')) \leq t'$. Thus **(Phy2)** holds.

- $E_{\varphi_i}(\sigma_i, t') = \sigma_{Si} \cdot (\delta + \delta', a) \neq \epsilon$ and at time $(t' + \delta')$, $E_{\varphi_i}(\sigma_i, t' + \delta') \models \varphi_i$. Hence **(Snd)** is satisfied.
- From Def. 3.6, K of E_{φ_i} gives the delayed word of $\sigma_{Ci} \cdot (\delta, a)$. Thus, **(Tr)** is satisfied and it is the minimal timed word according to the lexical order among the timed words with minimal duration ($\min_{\preceq_{lex,time}} K$), thus **(Op)** is also satisfied.

Now, this output is fed to E_{φ_j} at time t' and it makes a transition $t' = (l_j, \epsilon, a, Y_j, l'_j)$.
Let there be two cases on whether $K = \emptyset$ of E_{φ_j} or not.

Case 1a: $K \neq \emptyset$ of $E_{\varphi_j}(l'_j \in F)$
σ_{Cj} would necessarily be empty (i.e., $\sigma_{Cj} = \epsilon$), since φ_j is a safety property.
Hence, $E_{\varphi_j}(\sigma_j, t') = \sigma_{Sj} \cdot (\delta + \delta', a)$ (from Def. 3.6)

- $E_{\varphi_j}(\sigma_j, t) = \sigma_{Sj}$ and $E_{\varphi_j}(\sigma_j, t') = \sigma_{Sj} \cdot (\delta + \delta', a)$ and $t' \geq t$. Thus, **(Phy1)** is satisfied.
- $E_{\varphi_j}(\sigma_j, t') = \text{obs}\Big(\Pi_1\big(\text{store}_{\varphi_j}(\text{obs}(\sigma_j, t'))\big), t'\Big)$ and from definition and property of obs that $\forall \sigma : \text{time}(\text{obs}(\sigma_j, t')) \leq t$ applied to $\Pi_1\big(\text{store}_{\varphi_j}(\text{obs}(\sigma_j, t'))\big)$, we can conclude that $\text{time}(E_{\varphi_j}(\sigma_j, t')) \leq t'$. Thus **(Phy2)** holds.
- $E_{\varphi_j}(\sigma_j, t') = \sigma_{Sj} \cdot (\delta + \delta', a) \neq \epsilon$ and $l'_j \in F$. At time $(t' + \delta') \geq t$, $E_{\varphi_j}(\sigma_j, t' + \delta') \models \varphi_j$. Hence **(Snd)** is satisfied.
- Since, $t' = (l_j, g_j, a, Y_j, l'_j)$ where $g_j = \epsilon$, thus no delaying. **(Tr)** and **(Op)** are satisfied.

Thus, E_{φ_j} satisfies all defined constraints.

Case 1b: $K = \emptyset$ of $E_{\varphi_j}(l'_j \notin F)$
$E_{\varphi_j}(\sigma_j, t') = E_{\varphi_j}(\sigma_j, t) = \sigma_{Sj}$, with the event being delayed in buffer (from Def. 3.6).

- $E_{\varphi_j}(\sigma_j, t) = \sigma_{Sj}$ and $E_{\varphi_j}(\sigma_j, t') = \sigma_{Sj}$ and $t' \geq t$. Thus, **(Phy1)** is satisfied.
- $E_{\varphi_j}(\sigma_j, t') = \text{obs}\Big(\Pi_1\big(\text{store}_{\varphi_j}(\text{obs}(\sigma_j, t'))\big), t'\Big)$ and from definition and property of obs that $\forall \sigma : \text{time}(\text{obs}(\sigma_j, t')) \leq t$ applied to $\Pi_1\big(\text{store}_{\varphi_j}(\text{obs}(\sigma_j, t'))\big)$, we can conclude that $\text{time}(E_{\varphi_j}(\sigma_j, t')) \leq t'$. Thus **(Phy2)** holds.
- At time t, $E_{\varphi_j}(\sigma_j, t) \models \varphi_j$ and $E_{\varphi_j}(\sigma_j, t') = E_{\varphi_j}(\sigma_j, t)$. So, at time t', $E_{\varphi_j}(\sigma_j, t') \models \varphi_j$. Hence **(Snd)** is satisfied
- Since, no event is released, **(Tr)** and **(Op)** trivially holds.

Case 2: $K = \emptyset$ of E_{φ_i} (meaning we are not able to find a timed word, by appropriately delaying $\sigma_{Ci} \cdot (\delta, a)$ s.t. φ_i is satisfied)
where $(v + \delta + \delta') \not\models g_i$ or $l'_i \notin F$.
$E_{\varphi_i}(\sigma_i, t') = E_{\varphi_i}(\sigma_i, t) = \sigma_{Si} \cdot \epsilon$ (from Def. 3.6)
Similar to Case 1b, we can say that $E_{\varphi_i}(\sigma_i, t')$ satisfies the constraints at time t'.
And when the output from E_{φ_i} (i.e. ϵ) is fed to E_{φ_j} at time t', $E_{\varphi_j}(\sigma_j, t') = E_{\varphi_j}(\sigma_j, t) = \sigma_{Sj} \cdot \epsilon$, then again following Case 1b, we can say that $E_{\varphi_j}(\sigma_j, t')$ satisfies the constraints at time t'.

Thus, since all the constraints are satisfied by $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$, thus Proposition 1 holds for syntactic condition (a).

Considering syntactic condition (b) of Def. 4.5

Case 1: $K \neq \emptyset$ of E_{φ_i}
where $(v + \delta + \delta') \models g_i$ and $l'_i \in F$
σ_{Ci} would necessarily be empty (i.e., $\sigma_{Ci} = \epsilon$), since φ_i is a safety property.
Hence, $E_{\varphi_i}(\sigma_i, t') = \sigma_{Si} \cdot (\delta + \delta', a)$ (from Def. 3.6)

- $E_{\varphi_i}(\sigma_i, t) = \sigma_{Si}$ and $E_{\varphi_i}(\sigma_i, t') = \sigma_{Si} \cdot (\delta + \delta', a)$ and $t' \geq t$. Thus, **(Phy1)** is satisfied.
- $E_{\varphi_i}(\sigma_i, t') = \text{obs}\Big(\Pi_1\big(\text{store}_{\varphi_i}(\text{obs}(\sigma_i, t'))\big), t'\Big)$ and from definition and property of obs that $\forall \sigma : \text{time}(\text{obs}(\sigma_i, t')) \leq t$ applied to $\Pi_1\big(\text{store}_{\varphi_i}(\text{obs}(\sigma_i, t'))\big)$, we can conclude that $\text{time}(E_{\varphi_i}(\sigma_i, t')) \leq t'$. Thus **(Phy2)** holds.
- $E_{\varphi_i}(\sigma_i, t') = \sigma_{Si} \cdot (\delta + \delta', a) \neq \epsilon$ and at time $(t' + \delta')$, $E_{\varphi_i}(\sigma_i, t' + \delta') \models \varphi_i$. Hence **(Snd)** is satisfied.
- From Def. 3.6, K of E_{φ_i} gives the delayed word of $\sigma_{Ci} \cdot (\delta, a)$. Thus, **(Tr)** is satisfied and it is the minimal timed word according to the lexical order among the timed words with minimal duration ($\min \preceq_{lex,time} K$), thus **(Op)** is also satisfied.

Now, this output $(\delta + \delta', a)$ is fed to E_{φ_j} at time t'.
Let there be two cases on whether $K = \emptyset$ of E_{φ_j} or not.

Case 1a: $K \neq \emptyset$ of $E_{\varphi_j} (l'_j \in F)$
σ_{Cj} would necessarily be empty (i.e., $\sigma_{Cj} = \epsilon$), since, φ_j is a safety property.
Hence, $E_{\varphi_j}(\sigma_j, t') = \sigma_{Sj} \cdot (\delta + \delta' + \delta'', a)$ (from Def. 3.6)

- $E_{\varphi_j}(\sigma_j, t) = \sigma_{Sj}$ and $E_{\varphi_j}(\sigma_j, t') = \sigma_{Sj} \cdot (\delta + \delta' + \delta'', a)$ and $t' \geq t$. Thus, **(Phy1)** is satisfied.
- $E_{\varphi_j}(\sigma_j, t') = \text{obs}\Big(\Pi_1\big(\text{store}_{\varphi_j}(\text{obs}(\sigma_j, t'))\big), t'\Big)$ and from definition and property of obs that $\forall \sigma : \text{time}(\text{obs}(\sigma_j, t')) \leq t$ applied to $\Pi_1\big(\text{store}_{\varphi_j}(\text{obs}(\sigma_j, t'))\big)$, we can conclude that $\text{time}(E_{\varphi_j}(\sigma_j, t')) \leq t'$. Thus **(Phy2)** holds.
- $E_{\varphi_j}(\sigma_j, t') = \sigma_{Sj} \cdot (\delta + \delta' + \delta'', a) \neq \epsilon$ and $l'_j \in F$. At time $(t' + \delta' + \delta'') \geq t$, $E_{\varphi_j}(\sigma_j, t' + \delta' + \delta'') \models \varphi_j$. Hence **(Snd)** is satisfied.
- From Def. 3.6, K of E_{φ_j} gives the delayed word of $\sigma_{Cj} \cdot (\delta + \delta', a)$. Thus, **(Tr)** is satisfied and it is the minimal timed word according to the lexical order among the timed words with minimal duration ($\min \preceq_{lex,time} K$). Thus, **(Op)** is also satisfied.

Thus, E_{φ_j} satisfies all defined constraints.

Case 1b: $K = \emptyset$ of $E_{\varphi_j} (l'_j \notin F$ or $(v + \delta + \delta' + \delta'') \not\models g_i)$
$E_{\varphi_j}(\sigma_j, t') = E_{\varphi_j}(\sigma_j, t) = \sigma_{Sj}$ (from Def. 3.6), with the event being delayed in buffer (from Def. 3.6).

- $E_{\varphi_j}(\sigma_j, t) = \sigma_{Sj}$ and $E_{\varphi_j}(\sigma_j, t') = \sigma_{Sj}$ and $t' \geq t$. Thus, **(Phy1)** is satisfied.
- $E_{\varphi_j}(\sigma_j, t') = \text{obs}\Big(\Pi_1\big(\text{store}_{\varphi_j}(\text{obs}(\sigma_j, t'))\big), t'\Big)$ and from definition and property of obs that $\forall\sigma$: time(obs$(\sigma_j, t')) \leq t$ applied to $\Pi_1\big(\text{store}_{\varphi_j}(\text{obs}(\sigma_j, t'))\big)$, we can conclude that time$(E_{\varphi_j}(\sigma_j, t')) \leq t'$. Thus **(Phy2)** holds.
- At time t, $E_{\varphi_j}(\sigma_j, t) \models \varphi_j$ and $E_{\varphi_j}(\sigma_j, t') = E_{\varphi_j}(\sigma_j, t)$. So, at time t', $E_{\varphi_j}(\sigma_j, t') \models \varphi_j$. Hence **(Snd)** is satisfied
- Since, no event is released, **(Tr)** and **(Op)** trivially holds.

Case 2: $K = \emptyset$ of E_{φ_i}
where $(v + \delta + \delta') \not\models g_i$ or $l'_i \notin F$
$E_{\varphi_i}(\sigma_i, t') = E_{\varphi_i}(\sigma_i, t) = \sigma_{Si} \cdot \epsilon$ (from Def. 3.6)
Similar to Case 1b, we can say that $E_{\varphi_i}(\sigma_i, t')$ satisfies the constraints at time t'.
And when the output from E_{φ_i} (i.e. ϵ) is fed to E_{φ_j} at time t', $E_{\varphi_j}(\sigma_j, t') = E_{\varphi_j}(\sigma_j, t) = \sigma_{Sj} \cdot \epsilon$, then again following Case 1b, we can say that $E_{\varphi_j}(\sigma_j, t')$ satisfies the constraints at time t'.

Thus, since all the constraints are satisfied by $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$, thus Proposition 1 holds for syntactic condition (b).

Proposition 2 *(Output equivalence of the serial enforcer composed of the EMs of a set of safety TAs satisfying syntactic conditions given in Def. 4.5 w.r.t. the monolithic enforcer.) Consider a set of timed safety properties $\varphi_1, \varphi_2, \cdots, \varphi_n$ and their corresponding TAs $\mathcal{A}_{\varphi_1}, \mathcal{A}_{\varphi_2}, \cdots, \mathcal{A}_{\varphi_n}$ satisfying any condition in Def. 4.5. When the enforcers are combined serially as $E_{\varphi_1} \Rrightarrow E_{\varphi_2} \Rrightarrow \cdots \Rrightarrow E_{\varphi_n}$ (as per Def. 4.2), then, for any σ at time t, the output of the combined enforcer, is equal to the output of the monolithic enforcer, i.e., $E_{\varphi_1} \Rrightarrow E_{\varphi_2} \Rrightarrow \cdots \Rrightarrow E_{\varphi_n}(\sigma, t) = E_{\varphi_1 \cap \varphi_2 \cap \cdots \cap \varphi_n}(\sigma, t)$.*

Proposition 2 talks about the output equivalence of the serial enforcer w.r.t. the monolithic enforcer. It says that the serial enforcer composed out of properties whose safety TAs satisfy any condition in Def. 4.5 is output equivalent to the monolithic enforcer.

Proof: Let there be two properties φ_i and φ_j (the proof will generalize to any number of properties) and let their enforcers be connected in series as $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$.
Let their corresponding monolithic enforcer be $E_{\varphi_i \cap \varphi_j}$.
Let at time t, input given to them be σ.
Let at time $t'(= t + \delta)$, an action a arrives, thus input event is (δ, a).

Induction basis:
If $\sigma = \epsilon$ at time $t^0 (t^0 < t)$,
<u>For Serial enforcer:</u>
The considered transition in $\mathcal{A}_{\varphi_i}$ is $t_i = (l_i, g_i, \epsilon, Y_i, l'_i)$, $E_{\varphi_i}(\epsilon, t^0) = \epsilon$ (from Def.

3.6)
which is given to E_{φ_j} at time t^0
The considered transition in $\mathcal{A}_{\varphi_j}$ is $t_j = (l_j, g_j, \epsilon, Y_j, l'_j), E_{\varphi_j}(\epsilon, t^0) = \epsilon$ (from Def. 3.6)
Thus, $(E_{\varphi_i} \Rrightarrow E_{\varphi_j})(\epsilon, t^0) = \epsilon$.
<u>For Monolithic enforcer:</u>
The corresponding transition in $\mathcal{A}_{\varphi_i \cap \varphi_j}$ is $t_m = (l_m, g_m, \epsilon, Y_m, l'_m)$, $E_{\varphi_i \cap \varphi_j}(\epsilon, t^0) = \epsilon$ (from Def. 3.6)
Since, $(E_{\varphi_i} \Rrightarrow E_{\varphi_j})(\epsilon, t^0) = E_{\varphi_i \cap \varphi_j}(\epsilon, t^0)$, hence, Proposition 2 trivially holds for $\sigma = \epsilon$.

Induction step:
Assume that the proposition holds at time t when input is σ.
Now, let us prove that the proposition holds for $\sigma \cdot (\delta, a)$ at time t'.

Considering syntactic condition (a) of Def. 4.5
As we have seen in proof of Proposition 1 at 1, there will be 4 cases:

Case 1: $K \neq \emptyset$ of E_{φ_i} and $K \neq \emptyset$ of E_{φ_j}
Let $t_i = (l_i, g_i, a, Y_i, l'_i \in F_i), t_j = (l_j, \epsilon, a, Y_j, l'_j \in F_j)$

(a) Let $v + \delta \models g_i$
No delay is introduced by K of E_{φ_i} (as the current clock valuation satisfy the guards), and thus (δ, a) will be released as an output by $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$.
<u>For Monolithic enforcer:</u>
The corresponding transition in $\mathcal{A}_{\varphi_i \cap \varphi_j}$ is $t_m = (l_m, g_i, a, Y_m, l'_m)$, and since $(v + \delta) \models g_i$, thus, the output released by $E_{\varphi_i \cap \varphi_j}$ will be (δ, a).
Thus, the proposition holds.

(b) Let $v + \delta \not\models g_i$
Thus, delay is introduced by K of E_{φ_i} (as the current clock valuation does not satisfy the guards), and thus $(\delta + \delta', a)$ will be released as an output by $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$, where δ' will be the minimum delay (as per the optimality constraint) s.t. $(v + \delta + \delta') \models g_i$.
<u>For Monolithic enforcer:</u>
The corresponding transition in $\mathcal{A}_{\varphi_i \cap \varphi_j}$ is $t_m = (l_m, g_i, a, Y_m, l'_m)$, and since $(v + \delta) \not\models g_i$, the enforcer will introduce minimum delay (as per the optimality constraint) δ_m s.t. $(v + \delta + \delta_m) \models g_i$.
Thus, the output released by $E_{\varphi_i \cap \varphi_j}$ will be $(\delta + \delta_m, a)$.
Essentially $\delta' = \delta_m$, thus the proposition holds.

Case 2: $K \neq \emptyset$ of E_{φ_i} and $K = \emptyset$ of E_{φ_j}
Let $t_i = (l_i, g_i, a, Y_i, l'_i \in F_i), t_j = (l_j, \epsilon, a, Y_j, l'_j \notin F_j)$.
The output released by $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$ will be ϵ (the second enforcer in series will store the incoming event in its buffer and will not output anything as the state reached is not an accepting state).
<u>For Monolithic enforcer:</u>
The corresponding transition in $\mathcal{A}_{\varphi_i \cap \varphi_j}$ is $t_m = (l_m, g_i, a, Y_m, l'_m \notin F_m)$.
Thus, the output released by $E_{\varphi_i \cap \varphi_j}$ will be ϵ.
Thus, the proposition holds.

Case 3: $K = \emptyset$ of E_{φ_i} and $K \neq \emptyset$ of E_{φ_j}

Let $t_i = (l_i, g_i, a, Y_i, l'_i), t_j = (l_j, \epsilon, a, Y_j, l'_j \in F_j)$,
where $(\nexists \delta' : v + \delta' \models g_i) \mid\mid l'_i \notin F_i$
The output released by $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$ will be ϵ.
For Monolithic enforcer:
The corresponding transition in $\mathcal{A}_{\varphi_i \cap \varphi_j}$ is $t_m = (l_m, g_i, a, Y_m, l'_m)$.
Where $(\nexists \delta_m : v + \delta_m \models g_i) \mid\mid l'_m \notin F_m$
Thus, the output released by $E_{\varphi_i \cap \varphi_j}$ will be ϵ.
Thus, the proposition holds.

Case 4: $K = \emptyset$ of E_{φ_i} and $K = \emptyset$ of E_{φ_j}

Following above two cases, The output released by $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$ and $E_{\varphi_i \cap \varphi_j}$ will be ϵ.
Thus, the proposition holds.

Considering syntactic condition (b) of Def. 4.5

As we have seen in proof of Proposition 1 at 1, there will be 4 cases:

Case 1: $K \neq \emptyset$ of E_{φ_i} and $K \neq \emptyset$ of E_{φ_j}

Let $t_i = (l_i, g_i, a, Y_i, l'_i \in F_i), t_j = (l_j, g_j, a, Y_j, l'_j \in F_j)$

(a) Let $v + \delta \models g_i$
Thus, no delay introduced by K of E_{φ_i}.
Output of E_{φ_i} will be (δ, a) which is fed to E_{φ_j}.

i. Let $v + \delta \models g_j$
Thus, no delay introduced by K of E_{φ_j}.
Output of $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$ will be (δ, a).
For Monolithic enforcer:
The corresponding transition in $\mathcal{A}_{\varphi_i \cap \varphi_j}$ is $t_m = (l_m, g_i \cap g_j, a, Y_m, l'_m \in F_m)$, and since $(v + \delta) \models g_i \cap g_j$, thus, the output released by $E_{\varphi_i \cap \varphi_j}$ will be (δ, a).
Thus, the proposition holds.

ii. Let $v + \delta \not\models g_j$
Thus, delay δ' is introduced by K of E_{φ_j}.
Output of $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$ will be $(\delta + \delta', a)$.
For Monolithic enforcer:
The corresponding transition in $\mathcal{A}_{\varphi_i \cap \varphi_j}$ is $t_m = (l_m, g_i \cap g_j, a, Y_m, l'_m)$, and since $(v + \delta) \not\models g_i \cap g_j$, the enforcer will introduce minimum delay (as per the optimality constraint) δ_m s.t. $(v + \delta + \delta_m) \models g_i \cap g_j$ (δ_m is introduced to satisfy g_j of $g_i \cap g_j$).
Thus, the output released by $E_{\varphi_i \cap \varphi_j}$ will be $(\delta + \delta_m, a)$.
Essentially $\delta' = \delta_m$, thus, the proposition holds.

(b) Let $v + \delta \not\models g_i$
Thus, delay δ' is introduced by K of E_{φ_i}.
Output of E_{φ_i} will be $(\delta + \delta', a)$ which is fed to E_{φ_j}.

i. Let $v + \delta \models g_j$
Thus, no delay introduced by K of E_{φ_j}.
Output of $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$ will be $(\delta + \delta', a)$.
For Monolithic enforcer:
The corresponding transition in $\mathcal{A}_{\varphi_i \cap \varphi_j}$ is $t_m = (l_m, g_i \cap g_j, a, Y_m, l'_m \in$

F_m), and since $(v+\delta) \not\models g_i \cap g_j$, the enforcer will introduce minimum delay (as per the optimality constraint) δ_m s.t. $(v + \delta + \delta_m) \models g_i \cap g_j$ (δ_m is introduced to satisfy g_i of $g_i \cap g_j$).
Thus, the output released by $E_{\varphi_i \cap \varphi_j}$ will be $(\delta + \delta_m, a)$.
Essentially $\delta' = \delta_m$, thus the proposition holds.

ii. Let $v + \delta \not\models g_j$
Thus, delay δ'' is introduced by K of E_{φ_j}.
Output of $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$ will be $(\delta + \delta' + \delta'', a)$.
For Monolithic enforcer:
The corresponding transition in $\mathcal{A}_{\varphi_i \cap \varphi_j}$ is $t_m = (l_m, g_i \cap g_j, a, Y_m, l'_m \in F_m)$, and since $(v+\delta) \not\models g_i \cap g_j$, the enforcer will introduce minimum delay (as per the optimality constraint) δ_m s.t. $(v + \delta + \delta_m) \models g_i \cap g_j$.
Thus, the output released by $E_{\varphi_i \cap \varphi_j}$ will be $(\delta + \delta_m, a)$.
δ_m is essentially equal to $\delta' + \delta''$, thus, the proposition holds.

Case 2: $K \neq \emptyset$ of E_{φ_i} and $K = \emptyset$ of E_{φ_j}

Case 3: $K = \emptyset$ of E_{φ_i} and $K \neq \emptyset$ of E_{φ_j}

Case 4: $K = \emptyset$ of E_{φ_i} and $K = \emptyset$ of E_{φ_j}

Above cases 2,3,4 are similar to cases 2,3,4 for syntactic condition (a) where the output of $E_{\varphi_i \cap \varphi_j}$ and $E_{\varphi_i} \Rrightarrow E_{\varphi_j}$ will be ϵ. Thus, the proposition holds.

2 Example showing Evolution of the Enforcement function in Def. 3.6

Consider property P defined by the TA $\mathcal{A}_P$ in Fig. 1, with A as the initial and only accepting location. Let us see an example (Example 1) of evolution of the enforcement function for the property P.

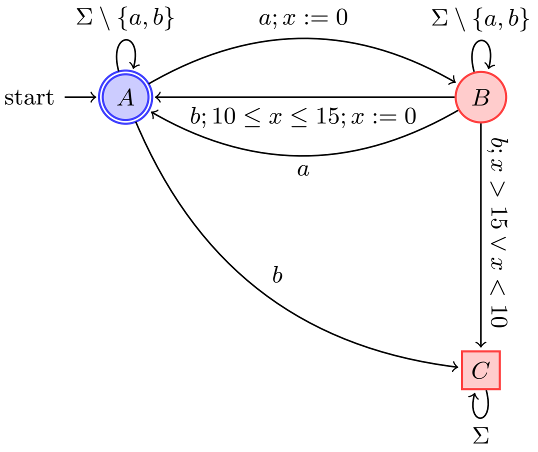

$\Sigma \setminus \{a, b\}$
$a; x := 0$
$\Sigma \setminus \{a, b\}$
start
A
B
$b; 10 \leq x \leq 15; x := 0$
a
b
$b; x > 15 \vee x < 10$
C
Σ

Figure 1: $\mathcal{A}_P$

Example 1 *(Evolution of the Enforcement function.) Consider* $\sigma = (3, a) \cdot (10, b) \cdot (3, a) \cdot (5, a)$ *to be the input timed word for the enforcer for* $\mathcal{A}_P$. *Tab. 1 shows the evolution of* obs, $\mathrm{store}_{\mathcal{A}_\mathrm{P}}$ *and* $E_{\mathcal{A}_P}$ *over time for input* σ. *The resulting output is* $(13, a) \cdot (15, b)$ *which satisfies property* P.

Table 1: Evolution of the enforcement function for property P

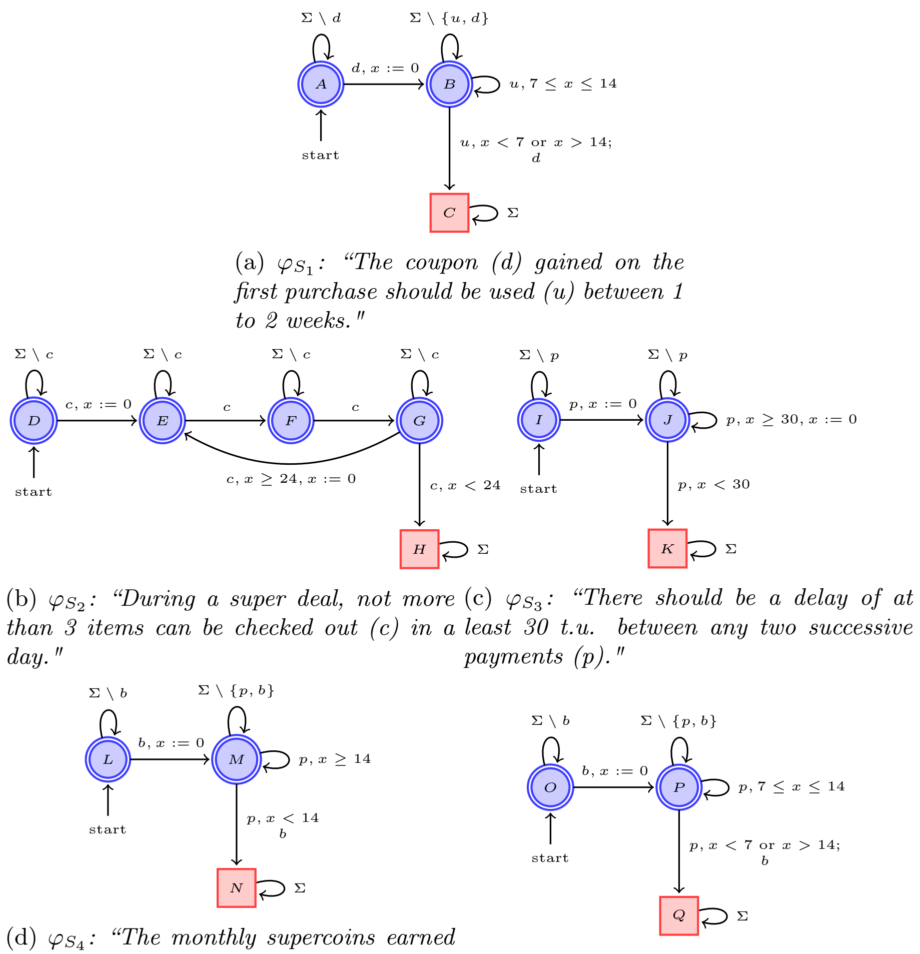
$t \in [0, 3)$	$\mathrm{obs}(\sigma, \mathrm{t}) = \epsilon$ $\mathrm{store}_{\mathcal{A}_\mathrm{P}}(\mathrm{obs}(\sigma, \mathrm{t})) = (\epsilon, \epsilon)$ $E_{\mathcal{A}_P}(\sigma, t) = \mathrm{obs}(\epsilon, \mathrm{t})$
$t \in [3, 13)$	$\mathrm{obs}(\sigma, \mathrm{t}) = (3, a)$ $\mathrm{store}_{\mathcal{A}_\mathrm{P}}(\mathrm{obs}(\sigma, \mathrm{t})) = (\epsilon, (3, a))$ $E_{\mathcal{A}_P}(\sigma, t) = \mathrm{obs}(\epsilon, t)$
$t \in [13, 16)$	$\mathrm{obs}(\sigma, \mathrm{t}) = ((3, a) \cdot (10, b))$ $\mathrm{store}_{\mathcal{A}_\mathrm{P}}(\mathrm{obs}(\sigma, \mathrm{t})) = ((13, a) \cdot (15, b), \epsilon)$ $E_{\mathcal{A}_P}(\sigma, t) = \mathrm{obs}((13, a) \cdot (15, b), t)$
$t \in [16, 21)$	$\mathrm{obs}(\sigma, \mathrm{t}) = ((3, a) \cdot (10, b) \cdot (3, a))$ $\mathrm{store}_{\mathcal{A}_\mathrm{P}}(\mathrm{obs}(\sigma, \mathrm{t})) = ((13, a) \cdot (15, b), (3, a))$ $E_{\mathcal{A}_P}(\sigma, t) = \mathrm{obs}((13, a) \cdot (15, b), t)$
$t \in [21, \infty)$	$\mathrm{obs}(\sigma, \mathrm{t}) = (3, a) \cdot (10, b) \cdot (3, a) \cdot (5, a)$ $\mathrm{store}_{\mathcal{A}_\mathrm{P}}(\mathrm{obs}(\sigma, \mathrm{t})) = ((13, a) \cdot (15, b), (3, a) \cdot (5, a))$ $E_{\mathcal{A}_P}(\sigma, t) = \mathrm{obs}((13, a) \cdot (15, b)), t)$

3 Formal runtime monitoring approaches in a non-critical systems: e-commerce company

Consider the scenario of an e-commerce company. Let there be the following safety timed properties φ_{S_1}, φ_{S_2}, φ_{S_3}, φ_{S_4} and φ_{S_5}:

- *"The coupon (d) gained on the first purchase should be used (u) between 1 to 2 weeks"*,
- *"During a super deal, not more than 3 items can be checked out (c) in a day"*,
- *"There should be a delay of at least 30 t.u. between any two successive payments (p)"*,
- *"The monthly supercoins earned (b) (from any number of purchases in a month) can be used (p) after the exchange period of all purchaces is over"*, and
- *"The promotional cashback (b) should be utilized (p) between 7 to 14 t.u."*.

respectively in an e-commerce company for smooth functioning of marketing, finance and supply chain. Fig. 2 shows their corresponding TAs.



(a) φ_{S_1}: *"The coupon (d) gained on the first purchase should be used (u) between 1 to 2 weeks."*

(b) φ_{S_2}: *"During a super deal, not more than 3 items can be checked out (c) in a day."*

(c) φ_{S_3}: *"There should be a delay of at least 30 t.u. between any two successive payments (p)."*

(d) φ_{S_4}: *"The monthly supercoins earned (b) (from any number of purchases in a month) can be used (p) after the exchange period of all purchaces is over."*

(e) φ_{S_5}: *"The promotional cashback (b) should be utilized (p) between 7 to 14 t.u.."*

Figure 2: Safety timed properties