Chapter 9

Composing the Overspeed and Collision Avoidance Protection Systems

In the previous chapters, we presented example protectors whose correct operation required that the physical plant automaton at hand satisfied particular properties. For instance, in the case of the VEHICLES automaton of Chapter 4, the overspeed protector OS-PROT of Chapter 5 assumes that none of the vehicles collide among themselves and the collision protector CL-PROT of Chapter 6 assumes that none of the vehicles exceed the speed limit. Similarly, the MERGE-PROT protector of Chapter 7 and the GRAPH-PROT protector of Chapter 8 guarantee that none of the vehicles collide among themselves in the MERGE-VEHICLES and GRAPH-VEHICLES automata, respectively, provided that all the vehicles are abiding by the speed limit. In this chapter, we compose the overspeed and collision protectors for the VEHICLES automaton and show that the resulting protector guarantees that the vehicles in the VEHICLES automaton neither exceed the speed limit, nor collide among themselves. We extend these results to the MERGE-VEHICLES and GRAPH-VEHICLES automata after assuming that the overspeed protector OS-PROT of Chapter 5 extends, virtually unchanged, to the MERGE-VEHICLES and GRAPH-VEHICLES automata.

9.1 Overspeed and Collision Avoidance for the VEHICLES Automaton

In the following lemma, we show that the composition of the protectors OS-PROT and CL-PROT guarantees that the vehicles in the VEHICLES automaton neither exceed the speed limit, nor collide among themselves.

Lemma 9.1.1 *The composition of* OS-PROT *and* CL-PROT *is a protector that guarantees* $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$ *in the* VEHICLES *automaton starting from* $S_{\text{OS-PROT}} \cap S_{\text{CL-PROT}}$.

In the following proof, we show that all the states of an execution of $PP \times$OS-PROT$\times$CL-PROT starting from $S_{\text{OS-PROT}} \cap S_{\text{CL-PROT}}$ are in $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$. This is done by applying Theorem 3.1.7 and showing that the second condition of the theorem does not hold.

Proof: Let α be any execution of the system $PP \times$ OS-PROT $\times$ CL-PROT starting from a state in $S_{\text{OS-PROT}} \cap S_{\text{CL-PROT}}$.

From Theorem 3.1.7, one of the following holds:

1. Every state in α is in $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$.
2. α can be written as $\alpha_1 \frown \alpha_2$, where
   (a) All state occurrences in α_1 except possibly the last are in $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$.
   (b) The last state occurrence in α_1 is in G_i, for some $i \in \{\text{OS-PROT}, \text{CL-PROT}\}$, if and only it is in $G_{i'}$, for $i' \in \{\text{OS-PROT}, \text{CL-PROT}\}, i' \neq i$.
   (c) All state occurrences in α_2 except possibly the first state occurrence of α_2 are in $\mathit{past}(\overline{G_{\text{OS-PROT}}}, \alpha) \cap \mathit{past}(\overline{G_{\text{CL-PROT}}}, \alpha)$.

We proceed by showing that it is not possible to decompose α into α_1 and α_2 as proposed by the second clause of Theorem 3.1.7. Then it trivially follows that the first clause of Theorem 3.1.7 holds; that is, for any such α, all states are in $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$.

The violation of $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$ can occur through the violation of either $G_{\text{OS-PROT}}$, or $G_{\text{CL-PROT}}$. On one hand, provided that no collisions have occurred, the violation of $G_{\text{OS-PROT}}$ can only occur within a trajectory of the VEHICLES automaton. On the other hand, the violation of $G_{\text{CL-PROT}}$ can only occur through the execution of a `colliding-pair`(i, i') action, for some $i, i' \in I, i' \neq i$. We analyze each of these cases separately.

1. In the first case, the key point is that the violation of the speed limit by any of the vehicles in the VEHICLES automaton can only occur within a trajectory and that a collision can not be recorded within a trajectory. Therefore, the fact that the speed limit is violated prior to the occurrence of any vehicle collisions would imply that the OS-PROT protector is not working correctly; that is, Corollary 5.3.1 is false.

   Let w be the first trajectory in α containing a state occurrence in $\overline{G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}}$. Suppose that w is a T_I-trajectory and let T'_I be the subset of T_I consisting of all t such that $(i, t, w(t)) \in \mathit{past}(\overline{G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}}, \alpha)$. Then T'_I is a non-empty subinterval of T_I that is "upward-closed", *i.e.*, if $t \in T'_I$, $t' \in T_I$, and $t < t'$, then $t' \in T'_I$. Since T'_I is an interval of reals, it has a left endpoint t which might or might not itself be in T'_I. It is important to note that since the $collided(i, i')$ variables, for $i, i' \in I, i \neq i'$, remain constant throughout any trajectory of the VEHICLES automaton, it is only possible to violate the $G_{\text{OS-PROT}}$ condition within the trajectory w; that is, all the states in w are in the set $G_{\text{CL-PROT}}$. Therefore, letting $s = w(t)$, all state occurrences in α that precede the state occurrence (i, t, s) are in the set $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$. Now, we attempt to decompose α into α_1 and α_2.

(a) Suppose we split α at any state preceding the state (i, t, s). Then the state (i, t, s) is in α_2. Since (i, t, s) is in $G_{\text{CL-PROT}}$ and all states that precede the state (i, t, s) are in $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$, it is the case that $(i, t, s) \notin past(\overline{G_{\text{OS-PROT}}}, \alpha) \cap past(\overline{G_{\text{CL-PROT}}}, \alpha)$. Since the state (i, t, s) is not the first state in α_2, the third condition is violated. Therefore, this decomposition of α is not valid.

(b) Suppose we split α at the state (i, t, s) and suppose that the state (i, t, s) is not the last state of w. Then any state of the trajectory w that succeeds the state (i, t, s) is in α_2. Moreover, since all of the states in w are in $G_{\text{CL-PROT}}$, none of the states in w that succeed (i, t, s) are in $past(\overline{G_{\text{OS-PROT}}}, \alpha) \cap past(\overline{G_{\text{CL-PROT}}}, \alpha)$. Therefore, the third condition is violated and this decomposition of α is not valid.

(c) Suppose we split α at the state (i, t, s) and suppose that the state (i, t, s) is the last state of w. Then since w is the first trajectory in α containing an occurrence of a state in $\overline{G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}}$, it follows that $(i, t, s) \in \overline{G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}}$. Moreover, since all the states in w are in $G_{\text{CL-PROT}}$, it is the case that $(i, t, s) \in \overline{G_{\text{OS-PROT}}} \cap G_{\text{CL-PROT}}$. Therefore, the second condition is violated and this decomposition of α is not valid.

(d) Suppose we split α at a state s'' that succeeds the state (i, t, s). Let (i, t', s') be a state of the trajectory w that succeeds the state (i, t, s) and precedes the state s''. The state (i, t', s') is in α_1. By definition of T_I', it is the case that (i, t', s') is in $past(\overline{G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}}, \alpha)$. Therefore, the first condition is violated and this decomposition of α is not valid.

2. In the second case, the key point is that a collision can only be recorded by an action and that such an action can not cause the velocity of a vehicle to exceed the speed limit. Therefore, the fact that a collision among the vehicles occurs prior to the violation of the speed limit would imply that the CL-PROT protector is not working correctly, *i.e.*, Lemma 6.3.1 is false.

   Without loss of generality, suppose that the $G_{\text{CL-PROT}}$ condition is violated through a `colliding-pair`(i, i') action, for some $i, i' \in I, i' \neq i$. Let p and p' be the states of the system prior to and succeeding this `colliding-pair`(i, i') action, *i.e.*, $p, p' \in VALID$ such that $p \xrightarrow{\pi} p'$, where $\pi =$ `colliding-pair`(i, i'). Since the `colliding-pair`(i, i') action only sets the $collided(i, i')$ variable to `True`, it follows that the state p' is in the set $G_{\text{OS-PROT}} \bigcap \overline{G_{\text{CL-PROT}}}$. Now, we attempt to decompose α into α_1 and α_2.

(a) Suppose we split α at any state preceding the state p. Then the state p is in α_2. Since p' is the first state in $\overline{G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}}$, it is the case that all the states of α preceding p' are in the set $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$; that is, $p \notin \mathit{past}(\overline{G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}}, \alpha)$ and $p \notin \mathit{past}(\overline{G_{\text{OS-PROT}}}, \alpha) \cap \mathit{past}(\overline{G_{\text{CL-PROT}}}, \alpha)$. Since p is not the first state in α_2, the third condition is violated. Therefore, this decomposition of α is not valid.

(b) Suppose we split α at the state p. Then the state p' is in α_2. Since p' is the first state in $\overline{G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}}$, it is the case that all the states of α preceding p' are in the set $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$; that is, $p \notin \mathit{past}(\overline{G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}}, \alpha)$ and, moreover, $p \notin \mathit{past}(\overline{G_{\text{OS-PROT}}}, \alpha) \cap \mathit{past}(\overline{G_{\text{CL-PROT}}}, \alpha)$. Since p' follows from p in a single step and $p' \in G_{\text{OS-PROT}} \cap \overline{G_{\text{CL-PROT}}}$, it is the case that $p' \notin \mathit{past}(\overline{G_{\text{OS-PROT}}}, \alpha) \cap \mathit{past}(\overline{G_{\text{CL-PROT}}}, \alpha)$. Therefore, the third condition is violated and this decomposition of α is not valid.

(c) Suppose we split α at the state p'. Then p' is the last state of α_1 and the first state of α_2. Since $p' \in G_{\text{OS-PROT}} \bigcap \overline{G_{\text{CL-PROT}}}$, the second condition is violated. Therefore, this decomposition of α is not valid.

(d) Suppose we split α at any state succeeding p'. Then the state p' is in α_1. Since $p' \in G_{\text{OS-PROT}} \bigcap \overline{G_{\text{CL-PROT}}}$, the first condition is violated. Therefore, this decomposition of α is not valid.

Therefore, the execution α cannot be decomposed into any such α_1 and α_2. It follows that the first clause of Theorem 3.1.7 must hold; that is, every state in α is in $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$. This implies that the protector OS-PROT $\times$ CL-PROT guarantees $G_{\text{OS-PROT}} \cap G_{\text{CL-PROT}}$ in the VEHICLES automaton starting from $S_{\text{OS-PROT}} \cap S_{\text{CL-PROT}}$. ∎

9.2 Overspeed and Collision Avoidance for the MERGE-VEHICLES Automaton

In the following lemma, we state that the composition of the protectors OS-PROT and MERGE-PROT guarantees that the vehicles of the MERGE-VEHICLES automaton neither exceed the speed limit, nor collide among themselves. It is important to note that it is assumed without proof that the protector OS-PROT and the Corollary 5.3.1 extend to the MERGE-VEHICLES automaton. In fact, since the strategy of the OS-PROT protector defined for the VEHICLES automaton in Chapter 5 does not depend on the nature of the track topology, the OS-PROT protector of Chapter 5 extends to the MERGE-VEHICLES automaton virtually unchanged.

Lemma 9.2.1 *The composition of* OS-PROT *and* MERGE-PROT *is a protector that guarantees* $G_{\text{OS-PROT}} \cap G_{\text{MERGE-PROT}}$ *in the* MERGE-VEHICLES *automaton starting from* $S_{\text{OS-PROT}} \cap S_{\text{MERGE-PROT}}$.

Proof: This proof follows precisely the steps of the proof of Lemma 9.1.1. ■

9.3 Overspeed and Collision Avoidance for the GRAPH-VEHICLES Automaton

In the following lemma, we state that the composition of the protectors OS-PROT and GRAPH-PROT guarantees that the vehicles of the GRAPH-VEHICLES automaton neither exceed the speed limit, nor collide among themselves. It is important to note that it is assumed without proof that the protector OS-PROT and the Corollary 5.3.1 extend to the GRAPH-VEHICLES automaton. In fact, since the strategy of the OS-PROT protector defined for the VEHICLES automaton in Chapter 5 does not depend on the nature of the track topology, the OS-PROT protector of Chapter 5 extends to the GRAPH-VEHICLES automaton virtually unchanged.

Lemma 9.3.1 *The composition of* OS-PROT *and* GRAPH-PROT *is a protector that guarantees* $G_{\text{OS-PROT}} \cap G_{\text{GRAPH-PROT}}$ *in the* GRAPH-VEHICLES *automaton starting from* $S_{\text{OS-PROT}} \cap S_{\text{GRAPH-PROT}}$.

Proof: This proof follows precisely the steps of the proof of Lemma 9.1.1. ■