Automated Requirements Analysis for a Molecular Watchdog Timer

Samuel J. Ellis, Eric R. Henderson, Titus H. Klinge, James I. Lathrop, Jack H. Lutz, Robyn R. Lutz, Divita Mathur, and Andrew S. Miner

2014/04/25

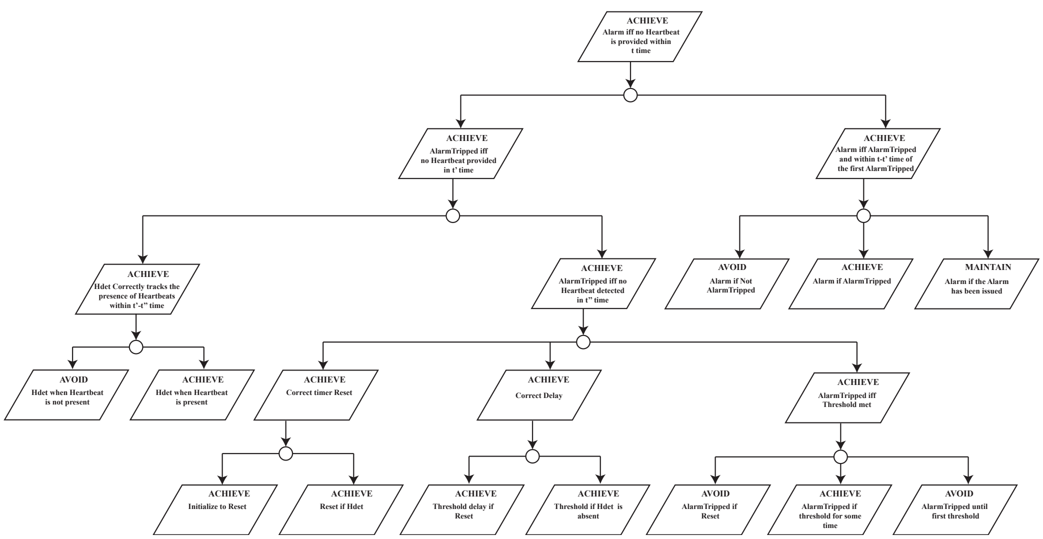

Figure 1: Goal Diagram Refinement

1 Proofs of Goal Diagram Implications

Lemma 1.1. The high-level goal is implied by its subgoals where

$$
\begin{array}{ll}
\mathcal{P}_{\geq 1-\epsilon}\Box_{\leq u}\neg A_{trip} & \wedge \\
\mathcal{P}_{\geq 1}\Box\left[H_{pres} \implies \mathcal{P}_{\geq 1-\epsilon_1}\Diamond_{\leq g}\left(\mathcal{P}_{\geq 1-\epsilon_2}\Box_{\leq u}\neg A_{trip}\right)\right] & \wedge \\
\mathcal{P}_{\geq 1}\Box\left[\neg H_{pres} \implies \mathcal{P}_{\geq 1-\delta_1}\Diamond_{\leq v-w_a}\left(A_{trip} \vee H_{pres}\right)\right] & \wedge \\
\mathcal{P}_{\geq 1}\Box\left[Alarm \implies \mathcal{P}_{\geq 1}\Box Alarm\right] & \wedge \\
\mathcal{P}_{\geq 1}\left(\neg Alarm\ \mathcal{W}\ A_{trip}\right) & \wedge \\
\mathcal{P}_{\geq 1}\Box\left[A_{trip} \implies \mathcal{P}_{1-\delta_2}\Diamond_{\leq w_a} Alarm\right] &
\end{array}
$$

is the high-level goal specification, and below are the subgoals:

Subgoal 1:

$$
\begin{array}{ll}
\mathcal{P}_{\geq 1-\epsilon}\Box_{\leq u}\neg A_{trip} & \wedge \\
\mathcal{P}_{\geq 1}\Box\left[H_{pres} \implies \mathcal{P}_{\geq 1-\epsilon_1}\Diamond_{\leq g}\left(\mathcal{P}_{\geq 1-\epsilon_2}\Box_{\leq u}\neg A_{trip}\right)\right] & \wedge \\
\mathcal{P}_{\geq 1}\Box\left[\neg H_{pres} \implies \mathcal{P}_{\geq 1-\delta_1}\Diamond_{\leq v-w_a}\left(A_{trip} \vee H_{pres}\right)\right] &
\end{array}
$$

Subgoal 2:

$$
\begin{array}{ll}
\mathcal{P}_{\geq 1}\Box\left[Alarm \implies \mathcal{P}_{\geq 1}\Box Alarm\right] & \wedge \\
\mathcal{P}_{\geq 1}\left(\neg Alarm\ \mathcal{W}\ A_{trip}\right) & \wedge \\
\mathcal{P}_{\geq 1}\Box\left[A_{trip} \implies \mathcal{P}_{1-\delta_2}\Diamond_{\leq w_a} Alarm\right] &
\end{array}
$$

Proof. Note that the first subgoal contains the first three statements of the parent goal and the second subgoal contains the last three. These six statements trivially compose the high-level goal if both are satisfied. $\square$

Lemma 1.2. The children of "**ACHIEVE:** AlarmTripped iff no HB provided in t' time" imply their parent where the parent specification is:

$$
\begin{array}{ll}
\mathcal{P}_{\geq 1-\epsilon}\Box_{\leq u}\neg A_{trip} & \wedge \quad (1) \\
\mathcal{P}_{\geq 1}\Box\left[H_{pres} \implies \mathcal{P}_{\geq 1-\epsilon_1}\Diamond_{\leq g}\left(\mathcal{P}_{\geq 1-\epsilon_2}\Box_{\leq u}\neg A_{trip}\right)\right] & \wedge \quad (2) \\
\mathcal{P}_{\geq 1}\Box\left[\neg H_{pres} \implies \mathcal{P}_{\geq 1-\delta_1}\Diamond_{\leq v-w_a}\left(A_{trip} \vee H_{pres}\right)\right] & \quad\ \ (3)
\end{array}
$$

and the subchildren are:

Subgoal 1:

$$\boldsymbol{\mathcal{P}}_{\geq 1}\Box\left[H_{pres} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\beta}\Diamond_{\leq w_h}\boldsymbol{\mathcal{P}}_{\geq 1-\alpha}H_{det}\right] \qquad \wedge \qquad (4)$$

$$\boldsymbol{\mathcal{P}}_{\geq 1}\Box\left[\neg H_{pres} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\beta}\Diamond_{w_h}\boldsymbol{\mathcal{P}}_{\geq 1-\alpha}\left(\neg H_{det}\ \boldsymbol{\mathcal{W}}\ H_{pres}\right)\right] \qquad (5)$$

Subgoal 2:

$$\boldsymbol{\mathcal{P}}_{\geq 1-\epsilon}\Box_{\leq u}\neg A_{trip} \qquad \wedge \qquad (6)$$

$$\boldsymbol{\mathcal{P}}_{\geq 1}\Box\left[H_{det} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\epsilon_1'}\Diamond_{\leq g-w_h}\left(\boldsymbol{\mathcal{P}}_{\geq 1-\epsilon_2'}\Box_{\leq u}\neg A_{trip}\right)\right] \qquad \wedge \qquad (7)$$

$$\boldsymbol{\mathcal{P}}_{\geq 1}\Box\left[\neg H_{det} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\delta_1'}\Diamond_{\leq v-w_a-w_h}\left(A_{trip} \vee H_{det}\right)\right] \qquad (8)$$

Proof. Assume that equations 1-3 true. We will now show that these five equations are sufficient to prove equations 1-3 each individually.

1. Equation (6) trivially implies (1).

2. In order to prove the implication in (2) holds, we assume that the boolean variable H_{pres} is true. By (4), with probability $(1-\beta)(1-\alpha)$, within w_h time, H_{det} will be true. When H_{det} is true, by (7), with probability $(1-\epsilon_1')(1-\epsilon_2')$, within $g-w_h$ time, $\neg A_{trip}$ becomes true. Thus, worst-case, with probability $(1-\alpha)(1-\beta)(1-\epsilon_1')(1-\epsilon_2')$, within g time, $\neg A_{trip}$ becomes true.

   Therefore, this implies the (2) if we enforce the constraints:

   - $1-\epsilon_1 \leq (1-\alpha)(1-\beta)(1-\epsilon_1')$
   - $1-\epsilon_2 \leq 1-\epsilon_2'$

3. Assume $\not H_{pres}$ is true. By (5), with probability $(1-\beta)(1-\alpha)$, within w_h time, $\neg H_{det}$ will be true until H_{pres} is true. Once $\neg H_{det}$ is true, by (8), with probability $(1-\delta_1')$, within $v-w_a-_w h$ time, we will either A_{trip} or H_{det}. Here we have two cases:

   Case 1: If *Atrip* happens within the appropriate time from $\neg H_{det}$ being true, then with probability $(1-\alpha)(1-\beta)(1-\delta_1')$, we will A_{trip} within $v-w_a$ time. This satisfies (3).

   Case 2: If *Atrip* does not happen within the appropriate time from H_{det} being true, then similarly, with probability $(1-\alpha)(1-\beta)(1-\delta_1')$, within $v-w_a$ time, H_{det} will become true. If H_{det} became true, then by (5) it must have been because H_{pres} became true. That means that H_{pres} became true in at most $v - w_a$ time and thus satisfies (3).

Therefore, the subchildren imply the parent if we enforce the constraints:

- $w_h \leq g$
- $1 - \epsilon_1 \leq (1-\alpha)(1-\beta)(1-\epsilon_1')$
- $1 - \epsilon_2 \leq 1 - \epsilon_2'$
- $1 - \delta_1 \leq (1-\alpha)(1-\beta)(1-\delta_1')$

$\square$

Lemma 1.3. The children of "**ACHIEVE:** Heartbeat Detected correctly tracks the presence of Heartbeats within $t' - t''$ time" imply their parent where the parent specification is:

$$\begin{aligned}&\boldsymbol{\mathcal{P}}_{\geq 1}\Box\left[H_{pres} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\beta}\Diamond_{\leq w_h}\boldsymbol{\mathcal{P}}_{\geq 1-\alpha}H_{det}\right] \qquad \wedge\\ &\boldsymbol{\mathcal{P}}_{\geq 1}\Box\left[\neg H_{pres} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\beta}\Diamond_{w_h}\boldsymbol{\mathcal{P}}_{\geq 1-\alpha}\left(\neg H_{det}\ \boldsymbol{\mathcal{W}}\ H_{pres}\right)\right]\end{aligned}$$

and the specification for the subgoals are:

Subgoal 1:

$$\boldsymbol{\mathcal{P}}_{\geq 1}\Box\left[\neg H_{pres} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\beta}\Diamond_{w_h}\boldsymbol{\mathcal{P}}_{\geq 1-\alpha}\left(\neg H_{det}\ \boldsymbol{\mathcal{W}}\ H_{pres}\right)\right]$$

Subgoal 2:

$$\boldsymbol{\mathcal{P}}_{\geq 1}\Box\left[H_{pres} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\beta}\Diamond_{\leq w_h}\boldsymbol{\mathcal{P}}_{\geq 1-\alpha}H_{det}\right]$$

Proof. It is clear that the children compose the parent and are equivalent. $\square$

Lemma 1.4. The children of "**ACHIEVE:** AlarmTripped iff no Heartbeat detected" imply their parent where the parent specification is:

$$\boldsymbol{\mathcal{P}}_{\geq 1-\epsilon}\Box_{\leq u}\neg A_{trip} \qquad \wedge \tag{9}$$

$$\boldsymbol{\mathcal{P}}_{\geq 1}\Box\left[H_{det} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\epsilon_1'}\Diamond_{\leq g-w_h}\left(\boldsymbol{\mathcal{P}}_{\geq 1-\epsilon_2'}\Box_{\leq u}\neg A_{trip}\right)\right] \qquad \wedge \tag{10}$$

$$\boldsymbol{\mathcal{P}}_{\geq 1}\Box\left[\neg H_{det} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\delta_1'}\Diamond_{\leq v-w_a-w_h}\left(A_{trip} \vee H_{det}\right)\right] \tag{11}$$

and the specification of the children are:

Subgoal 1:

$$\begin{aligned} &Reset && \wedge && (12)\\ &\boldsymbol{\mathcal{P}}_{\geq 1}\Box\,[H_{det} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\lambda_1}\Diamond_{\leq w_{on}} Reset] && && (13)\end{aligned}$$

Subgoal 2:

$$\begin{aligned} &\boldsymbol{\mathcal{P}}_{\geq 1}\Box\,[Reset \implies \boldsymbol{\mathcal{P}}_{\geq 1-\gamma_1}\Box_{\leq u} Th_L] && \wedge && (14)\\ &\boldsymbol{\mathcal{P}}_{\geq 1}\Box[\neg H_{det} \implies \boldsymbol{\mathcal{P}}_{\geq 1-\eta_1}\Diamond_{v-w_a-2w_h-w_{th}} \\ &\qquad \boldsymbol{\mathcal{P}}_{\geq 1-\eta_2}\,(Th_H\ \boldsymbol{\mathcal{W}}\ \boldsymbol{\mathcal{P}}_{\geq 1-\eta_3}\Diamond_{\leq w_h} H_{det})] && && (15)\end{aligned}$$

Subgoal 3:

$$\begin{aligned} &\boldsymbol{\mathcal{P}}_{\geq 1}\Box\,\left[Th_L \implies \boldsymbol{\mathcal{P}}_{\geq 1-\lambda_2}\Diamond_{\leq w_{off}}\boldsymbol{\mathcal{P}}_{\geq 1-\lambda_3}\Box_{\leq u}\neg A_{trip}\right] && \wedge && (16)\\ &\boldsymbol{\mathcal{P}}_{\geq 1}\Box\,[Th_H \implies \boldsymbol{\mathcal{P}}_{\geq 1-\eta_4}\Diamond_{\leq w_{th}}\,(A_{trip}\ \vee\ \neg Th_H)] && \wedge && (17)\\ &\boldsymbol{\mathcal{P}}_{\geq 1-\gamma_2}\,(\neg A_{trip}\ \boldsymbol{\mathcal{W}}\ \neg Th_L) && && (18)\end{aligned}$$

Proof. Assume the truth of equations 12-18. It suffices to show that equations 9-11 are true.

1. By (12), $Reset$ is true. By (14), with probabilitly $1-\gamma_1$, Th_L will be true for u time. By (18), $\neg A_{trip}$ will not be true until $\neg Th_L$ is true with probability $1-\gamma_2$. This implies (9) if the following constraint is met:
   - $1-\epsilon \leq (1-\gamma_1)(1-\gamma_2)$
2. Assume that H_{det} is true. By (13), witih probability $1-\lambda_1$, within w_{on} time, $Reset$ will be true. By (14), with probability $1-\gamma_1$, Th_L will be true for u time. By (17), with probability $1-\lambda_2$, within w_{off} time, with probability $1-\lambda_3$, we will $\neg A_{trip}$ for u time. This implies (10) if we enfore the following constraints:
   - $(1-\epsilon_1')(1-\epsilon_2') \leq (1-\lambda_1)(1-\gamma_1)(1-\lambda_2)(1-\lambda_3)$
   - $g-w_h \geq w_{on}+w_{off}$
3. Assume $\neg H_{det}$ is true. By (15), with at least $(1-\eta_1)(1-\eta_2)(1-\eta_3)$ probability, within $v-w_a-2w_h-w_{th}$ time, a path will enter a position that satisfies $Th_H\ \boldsymbol{\mathcal{W}}\ \Diamond_{w_h} H_{det}$. Thus we have two cases:

Case 1: Once Th_H becomes true, before w_{th} time passes, $\Diamond_{w_h} H_{det}$ becomes true. Therefore, in at most $v - w_a - w_h$ time, we receive an H_{det} and thus satisfy (11).

Case 2: Once Th_H becomes true, it stays true for at least w_{th} time. Then by (17), with probability $1 - \gamma_2$, within w_{th} time of Th_H becoming true, we will A_{trip} or $\neg Th_H$. Since we know Th_H is true for at least w_{th} time, we know we must A_{trip} by w_{th} time. Therefore, we have an A_{trip} in no later than $w - w_a - w_h$ time and satisfy (11).

The above cases only hold true if we enfore the following constraint:

- $1 - \delta_2 \leq (1 - \eta_1)(1 - \eta_2)(1 - \eta_3)(1 - \gamma_2)$

Because each of equations 9-11 hold true with our assumptions, it is clear our subgoals imply the parent. □

Lemma 1.5. All parent goals of leaves are implied by their children.

Proof. All leave goals are broken down by conjunction and trivially imply their parents. □

Theorem 1.6. All the leaf goals imply the high level goal of our goal diagram.

Proof. By all of the lemmas proven above, the leaves successfully imply the high level goal. □