Supplementary Materials for Compositional Probabilistic Analysis of Temporal Properties over Stochastic Detectors

Ivan Ruchkin, Oleg Sokolsky, James Weimer, Tushar Hedaoo, and Insup Lee.

***Abstract*—This supplement contains additional material for the article "Compositional Probabilistic Analysis of Temporal Properties over Stochastic Detectors" (by the same authors) from the ESWEEK-TCAD special issue, presented in the International Conference on Embedded Software 2020. The supplement contains the additional semantics, derivations, and visualizations.**

***Index Terms*—detection algorithms, probabilistic logic, formal languages, parameter estimation, cyber-physical systems**

Appendix

This is a supplement for the main paper, Compositional Probabilistic Analysis of Temporal Properties over Stochastic Detectors, which can be found in the special issue of IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems for the Embedded Systems Week 2020.

This document contains the following sections:

- Features of LTL$_{3d}$ (Appendix A)
- Full Definitions for Detector Compositions (Appendix B)
- Sufficiency of Defining Detector Events (Appendix C)
- Consistent Probability Extension in Multi-Detector Spaces (Appendix D)
- Independence of Detector Variables and Events (Appendix E)
- Logical Tautologies for Detectors (Appendix F)
- Rules for Probability Reasoning (Appendix G)
- Rules for Independence Reasoning (Appendix H)
- Full Derivation of Error Rate Formulas for Monitors (Appendix I)
- Additional Figures for Evaluation (Appendix J)

The implementation of the computational assistant, as well as the pipeline monitoring dataset, can be found at https://github.com/bisc/prob-comp-asst.

A. Features of LTL$_{3d}$

The 3-value linear temporal logic for detectors, LTL$_{3d}$, has the following features:

- Two interpretations: 3-value $[\![\![\,]\!]\!]$ and 2-value $[\![\,]\!]$. The former follows Kleene's strong logic [1], and the latter follows the classic binary LTL [2].
- Linear temporal modalities with time bounds.
- Three negation operators: $\neg_s$, $\neg_w$, and $\neg_{se}$.
- Finite traces, assumed to be sufficiently long to evaluate a given formula.

Syntactic sugar is defined based on its core syntax:

$$\begin{aligned}
\mathsf{F} &\equiv \neg_s \mathsf{T} \\
\varphi_1 \wedge \varphi_2 &\equiv \neg_s(\neg_s\varphi_1 \boldsymbol{\wedge} \neg_s\varphi_2) \\
\varphi_1 \rightarrow_s \varphi_2 &\equiv \neg_s\varphi_1 \boldsymbol{\vee} \varphi_2 \\
\varphi_1 \rightarrow_w \varphi_2 &\equiv \neg_w\varphi_1 \boldsymbol{\vee} \varphi_2 \\
\varphi_1 \rightarrow_{se} \varphi_2 &\equiv \neg_{se}\varphi_1 \boldsymbol{\vee} \varphi_2 \\
\Diamond_{[m,n]}\varphi &\equiv \mathsf{T}\, \boldsymbol{U}_{[m,n]}\, \varphi \\
\Box_{[m,n]}\varphi &\equiv \neg_s \Diamond_{[m,n]} \neg_s \varphi
\end{aligned} \tag{1}$$

B. Full Definitions for Detector Compositions

This section provides full expressions for the marginal events of composite detectors. All of these expressions form the list $\mathcal{R}_{\text{ev}}$ used in Step 1.2 of the analysis. In this section, superscripts indicate temporal or set indexing; subscripts indicate different detectors. Table I shows the events of common compositions.

Strong negation $\neg_s$:

$$\begin{align}
\text{gtt}(\neg_s \boldsymbol{D}) &= \text{gtf}(\boldsymbol{D}) \tag{2} \\
\text{gtf}(\neg_s \boldsymbol{D}) &= \text{gtt}(\boldsymbol{D}) \notag \\
\text{dot}(\neg_s \boldsymbol{D}) &= \text{dof}(\boldsymbol{D}) \tag{3} \\
\text{dof}(\neg_s \boldsymbol{D}) &= \text{dot}(\boldsymbol{D}) \notag \\
\text{dou}(\neg_s \boldsymbol{D}) &= \text{dou}(\boldsymbol{D}) \notag
\end{align}$$

Weak negation $\neg_w$:

$$\begin{align}
\text{gtt}(\neg_w \boldsymbol{D}) &= \text{gtf}(\boldsymbol{D}) \tag{4} \\
\text{gtf}(\neg_w \boldsymbol{D}) &= \text{gtt}(\boldsymbol{D}) \notag \\
\text{dot}(\neg_w \boldsymbol{D}) &= \text{dof}(\boldsymbol{D}) \vee \text{dou}(\boldsymbol{D}) \tag{5} \\
\text{dof}(\neg_w \boldsymbol{D}) &= \text{dot}(\boldsymbol{D}) \notag \\
\text{dou}(\neg_w \boldsymbol{D}) &= \mathsf{F} \notag
\end{align}$$

Strong exclusive negation $\neg_{se}$:

$$\begin{aligned}
\text{gtt}(\neg_{se} \boldsymbol{D}) &= \text{gtf}(\boldsymbol{D}) \\
\text{gtf}(\neg_{se} \boldsymbol{D}) &= \text{gtt}(\boldsymbol{D}) \\
\text{dot}(\neg_{se} \boldsymbol{D}) &= \text{dof}(\boldsymbol{D}) \\
\text{dof}(\neg_{se} \boldsymbol{D}) &= \text{dot}(\boldsymbol{D}) \vee \text{dou}(\boldsymbol{D}) \\
\text{dou}(\neg_{se} \boldsymbol{D}) &= \mathsf{F}
\end{aligned}$$

All the authors are with the Department of Computer and Information Science, University of Pennsylvania, Philadelphia, PA, USA. The first author can be contacted at iruchkin@cis.upenn.edu

Event	$\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b$	$\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b$	$\boldsymbol{\neg}_s \boldsymbol{D}$	$\boldsymbol{\neg}_w \boldsymbol{D}$	$\boldsymbol{\neg}_{se} \boldsymbol{D}$
$\mathrm{gtt}(\boldsymbol{D}')$	$\mathrm{gtt}(\boldsymbol{D}_a) \wedge \mathrm{gtt}(\boldsymbol{D}_b)$	$\mathrm{gtt}(\boldsymbol{D}_a) \vee \mathrm{gtt}(\boldsymbol{D}_b)$	$\mathrm{gtf}(\boldsymbol{D})$	$\mathrm{gtf}(\boldsymbol{D})$	$\mathrm{gtf}(\boldsymbol{D})$
$\mathrm{gtf}(\boldsymbol{D}')$	$\mathrm{gtf}(\boldsymbol{D}_a) \vee \mathrm{gtf}(\boldsymbol{D}_b)$	$\mathrm{gtf}(\boldsymbol{D}_a) \wedge \mathrm{gtf}(\boldsymbol{D}_b)$	$\mathrm{gtt}(\boldsymbol{D})$	$\mathrm{gtt}(\boldsymbol{D})$	$\mathrm{gtt}(\boldsymbol{D})$
$\mathrm{dot}(\boldsymbol{D}')$	$\mathrm{dot}(\boldsymbol{D}_a) \wedge \mathrm{dot}(\boldsymbol{D}_b)$	$\mathrm{dot}(\boldsymbol{D}_a) \vee \mathrm{dot}(\boldsymbol{D}_b)$	$\mathrm{dof}(\boldsymbol{D})$	$\mathrm{dof}(\boldsymbol{D}) \vee \mathrm{dou}(\boldsymbol{D})$	$\mathrm{dof}(\boldsymbol{D})$
$\mathrm{dof}(\boldsymbol{D}')$	$\mathrm{dof}(\boldsymbol{D}_a) \vee \mathrm{dof}(\boldsymbol{D}_b)$	$\mathrm{dof}(\boldsymbol{D}_b) \wedge \mathrm{dof}(\boldsymbol{D}_b)$	$\mathrm{dot}(\boldsymbol{D})$	$\mathrm{dot}(\boldsymbol{D})$	$\mathrm{dot}(\boldsymbol{D}) \vee \mathrm{dou}(\boldsymbol{D})$
$\mathrm{dou}(\boldsymbol{D}')$	$\mathrm{dou}(\boldsymbol{D}^1) \wedge \mathrm{dou}(\boldsymbol{D}^2) \vee$ $\mathrm{dou}(\boldsymbol{D}^1) \wedge \mathrm{dot}(\boldsymbol{D}^2) \vee$ $\mathrm{dou}(\boldsymbol{D}^2) \wedge \mathrm{dot}(\boldsymbol{D}^1)$	$\mathrm{dou}(\boldsymbol{D}^1) \wedge \mathrm{dou}(\boldsymbol{D}^2) \vee$ $\mathrm{dou}(\boldsymbol{D}^1) \wedge \mathrm{dof}(\boldsymbol{D}^2) \vee$ $\mathrm{dou}(\boldsymbol{D}^2) \wedge \mathrm{dof}(\boldsymbol{D}^1)$	$\mathrm{dou}(\boldsymbol{D})$	F	F

Table I: Detector compositions defined through the events of new detector $\boldsymbol{D}'$.

Conjunction $\boldsymbol{\wedge}$:

$$\begin{aligned}
\mathrm{gtt}(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b) &= \mathrm{gtt}(\boldsymbol{D}_a) \wedge \mathrm{gtt}(\boldsymbol{D}_b) && (6)\\
\mathrm{gtf}(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b) &= \mathrm{gtf}(\boldsymbol{D}_a) \vee \mathrm{gtf}(\boldsymbol{D}_b) \\
\mathrm{dot}(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b) &= \mathrm{dot}(\boldsymbol{D}_a) \wedge \mathrm{dot}(\boldsymbol{D}_b) && (7)\\
\mathrm{dof}(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b) &= \mathrm{dof}(\boldsymbol{D}_a) \vee \mathrm{dof}(\boldsymbol{D}_b) \\
\mathrm{dou}(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b) &= \mathrm{dou}(\boldsymbol{D}_a) \wedge \mathrm{dou}(\boldsymbol{D}_b) \ \vee \\
&\quad\ \mathrm{dou}(\boldsymbol{D}_a) \wedge \mathrm{dot}(\boldsymbol{D}_b) \ \vee \\
&\quad\ \mathrm{dou}(\boldsymbol{D}_b) \wedge \mathrm{dot}(\boldsymbol{D}_a)
\end{aligned}$$

Disjunction $\boldsymbol{\vee}$:

$$\begin{aligned}
\mathrm{gtt}(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b) &= \mathrm{gtt}(\boldsymbol{D}_a) \vee \mathrm{gtt}(\boldsymbol{D}_b), \\
\mathrm{gtf}(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b) &= \mathrm{gtf}(\boldsymbol{D}_a) \wedge \mathrm{gtf}(\boldsymbol{D}_b), \\
\mathrm{dot}(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b) &= \mathrm{dot}(\boldsymbol{D}_a) \vee \mathrm{dot}(\boldsymbol{D}_b), \\
\mathrm{dof}(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b) &= \mathrm{dof}(\boldsymbol{D}_a) \wedge \mathrm{dof}(\boldsymbol{D}_b), \\
\mathrm{dou}(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b) &= \mathrm{dou}(\boldsymbol{D}_a) \wedge \mathrm{dou}(\boldsymbol{D}_b) \ \vee \\
&\quad\ \mathrm{dou}(\boldsymbol{D}_a) \wedge \mathrm{dof}(\boldsymbol{D}_b) \ \vee \\
&\quad\ \mathrm{dou}(\boldsymbol{D}_b) \wedge \mathrm{dof}(\boldsymbol{D}_a)
\end{aligned}$$

Until $\boldsymbol{U}_{[m,n]}$:

$$\begin{aligned}
\mathrm{gtt}(\boldsymbol{D}_a \, \boldsymbol{U}_{[m,n]} \, \boldsymbol{D}_b) = \quad & \exists t \in [m..n] \cdot \mathrm{gtt}(\boldsymbol{D}_b^t) \wedge \mathrm{gtt}(\boldsymbol{D}_a^1) \wedge \ldots \\
& \wedge \mathrm{gtt}(\boldsymbol{D}_a^{t-1}) \\
\mathrm{gtf}(\boldsymbol{D}_a \, \boldsymbol{U}_{[m,n]} \, \boldsymbol{D}_b) = \quad & \big(\forall t \in [m..n] \cdot \mathrm{gtf}(\boldsymbol{D}_b^t)\big) \vee \\
& \big(\exists t \in [m..n] \cdot \mathrm{gtf}(\boldsymbol{D}_a^t) \wedge \mathrm{gtf}(\boldsymbol{D}_b^m) \wedge \ldots \\
& \wedge \mathrm{gtf}(\boldsymbol{D}_b^{t-1})\big) \\
\mathrm{dot}(\boldsymbol{D}_a \, \boldsymbol{U}_{[m,n]} \, \boldsymbol{D}_b) = \quad & \exists t \in [m..n] \cdot \mathrm{dot}(\boldsymbol{D}_b^t) \wedge \mathrm{dot}(\boldsymbol{D}_a^1) \wedge \ldots \\
& \wedge \mathrm{dot}(\boldsymbol{D}_a^{t-1}) \\
\mathrm{dof}(\boldsymbol{D}_a \, \boldsymbol{U}_{[m,n]} \, \boldsymbol{D}_b) = \quad & \big(\forall t \in [m..n] \cdot \mathrm{dof}(\boldsymbol{D}_b^t)\big) \vee \\
& \big(\exists t \in [m..n] \cdot \mathrm{dof}(\boldsymbol{D}_a^t) \wedge \mathrm{dof}(\boldsymbol{D}_b^m) \wedge \ldots \\
& \wedge \mathrm{dof}(\boldsymbol{D}_b^{t-1})\big) \\
\mathrm{dou}(\boldsymbol{D}_a \, \boldsymbol{U}_{[m,n]} \, \boldsymbol{D}_b) = \quad & \neg \, \mathrm{dot}(\boldsymbol{D}_a \, \boldsymbol{U}_{[m,n]} \, \boldsymbol{D}_b) \ \wedge \\
& \neg \, \mathrm{dof}(\boldsymbol{D}_a \, \boldsymbol{U}_{[m,n]} \, \boldsymbol{D}_b)
\end{aligned}$$

Always $\boldsymbol{\Box}_{[1,n]}$:

$$\begin{aligned}
\mathrm{gtt}(\boldsymbol{\Box}_{[1,n]} \boldsymbol{D}) &= \mathrm{gtt}(\boldsymbol{D}^1) \wedge \ldots \wedge \mathrm{gtt}(\boldsymbol{D}^n) \\
\mathrm{gtf}(\boldsymbol{\Box}_{[1,n]} \boldsymbol{D}) &= \mathrm{gtf}(\boldsymbol{D}^1) \vee \ldots \vee \mathrm{gtf}(\boldsymbol{D}^n) \\
\mathrm{dot}(\boldsymbol{\Box}_{[1,n]} \boldsymbol{D}) &= \mathrm{dot}(\boldsymbol{D}^1) \wedge \ldots \wedge \mathrm{dot}(\boldsymbol{D}^n) \\
\mathrm{dof}(\boldsymbol{\Box}_{[1,n]} \boldsymbol{D}) &= \mathrm{dof}(\boldsymbol{D}^1) \vee \ldots \vee \mathrm{dof}(\boldsymbol{D}^n) \\
\mathrm{dou}(\boldsymbol{\Box}_{[1,n]} \boldsymbol{D}) &= \bigvee_{S:\mathcal{P}(1..n)} \Big(\bigwedge_{i:S} \mathrm{dot}(\boldsymbol{D}^i) \bigwedge_{j:\mathcal{P}(1..n)\setminus S} \mathrm{dou}(\boldsymbol{D}^j)\Big)
\end{aligned}$$

where $\mathcal{P}\left(\right)$ stands for a powerset.

Eventually $\boldsymbol{\Diamond}_{[1,n]}$:

$$\begin{aligned}
\mathrm{gtt}(\boldsymbol{\Diamond}_{[1,n]} \boldsymbol{D}) &= \mathrm{gtt}(\boldsymbol{D}^1) \vee \ldots \vee \mathrm{gtt}(\boldsymbol{D}^n) \\
\mathrm{gtf}(\boldsymbol{\Diamond}_{[1,n]} \boldsymbol{D}) &= \mathrm{gtf}(\boldsymbol{D}^1) \wedge \ldots \wedge \mathrm{gtf}(\boldsymbol{D}^n) \\
\mathrm{dot}(\boldsymbol{\Diamond}_{[1,n]} \boldsymbol{D}) &= \mathrm{dot}(\boldsymbol{D}^1) \vee \ldots \vee \mathrm{dot}(\boldsymbol{D}^n) \\
\mathrm{dof}(\boldsymbol{\Diamond}_{[1,n]} \boldsymbol{D}) &= \mathrm{dof}(\boldsymbol{D}^1) \wedge \ldots \wedge \mathrm{dof}(\boldsymbol{D}^n) \\
\mathrm{dou}(\boldsymbol{\Diamond}_{[1,n]} \boldsymbol{D}) &= \bigvee_{S:\mathcal{P}(1..n)} \Big(\bigwedge_{i:S} \mathrm{dof}(\boldsymbol{D}^i) \bigwedge_{j:\mathcal{P}(1..n)\setminus S} \mathrm{dou}(\boldsymbol{D}^j)\Big)
\end{aligned}$$

Based on the above definitions, syntactic sugar for unary modal operators is part of $\mathcal{R}_{\text{log}}$:

$$\boldsymbol{\Box}_{[m,n]} \boldsymbol{D} ::= \boldsymbol{D}^m \boldsymbol{\wedge} \ldots \boldsymbol{\wedge} \boldsymbol{D}^n \qquad (8)$$

$$\boldsymbol{\Diamond}_{[m,n]} \boldsymbol{D} ::= \boldsymbol{D}^m \boldsymbol{\vee} \ldots \boldsymbol{\vee} \boldsymbol{D}^n \qquad (9)$$

C. Sufficiency of Defining Detector Events

Here we prove that a detector is unambiguously defined by its marginal events.

A detector is fully identified by its two random variables DO and GT. Therefore, to show that two detectors are identical, it is necessary and sufficient that their random variables always take the same values. The following proposition demonstates that all of the above definitions via events (gtt, gtf, dot, dof, and dou) unambiguously determine a detector, and hence no additional information is required.

Proposition 1. If arbitrary detectors $\boldsymbol{D}^1$ and $\boldsymbol{D}^2$ in the same space Ω have respectively co-occurring[1] events gtt, gtf, dot, dof, and dou, then their r.v.s DO^1 and DO^2, as well as GT^1 and GT^2, always take the same values.

Proof. Events gtt and gtf fully determine the values of GT^1 and GT^2. Since the events always co-occur, it follows that $GT^1 = GT^2$.

[1] Meaning that $\mathrm{gtt}(\boldsymbol{D}^1)$ occurs iff $\mathrm{gtt}(\boldsymbol{D}^2)$ occurs — and the same for the other four pairs of events.

Similarly, events dot, dof, and dou fully determine the values of GT^1 and GT^2. Therefore, from their co-occurrence it follows that always $DO^1 = DO^2$. □

D. Consistent Probability Extension in Multi-Detector Spaces

The multi-detector probability space $(\boldsymbol{\Omega}, \boldsymbol{\mathcal{F}}, \mathsf{Pr})$ has a discrete probability measure Pr that is extended from measures $\mathrm{Pr}^1 \dots \mathrm{Pr}^n$ of the individual detector spaces. This extension of Pr is largely undetermined a priori because it depends on how the r.v.s behave jointly; Pr is only constrained by the Kolmogorov axioms and consistency with the individual $\mathrm{Pr}^1 \dots \mathrm{Pr}^n$ measures on the events of individual detectors.

The consistency with between Pr and $\mathrm{Pr}^1 \dots \mathrm{Pr}^n$ requires that the latter measures of any marginal event $e_i \in \mathcal{F}^i$ (of the i-th detector, for any $i \in \{1 \dots n\}$) equal the Pr measure of this event's projection onto $\boldsymbol{\mathcal{F}}$:

$$\mathrm{Pr}^i(e_i) = \mathsf{Pr}(\{(\boldsymbol{\Omega}^1, \dots e_i \dots, \boldsymbol{\Omega}^n)\})$$

This requirement is satisfied by fixing $\boldsymbol{\Omega}$ in each specific case and addressing events in $\boldsymbol{\mathcal{F}}$ by their unique names (e.g., $\mathrm{dot}(\boldsymbol{D}^1)$), as we do in our notation.

E. Independence of Detector Variables and Events

The independence statement $GT^i \perp\!\!\!\perp GT^{i+1}$ is equivalent to the following four assertions:

$$\mathsf{Pr}(\mathrm{gtt}(\boldsymbol{D}^i) \wedge \mathrm{gtt}(\boldsymbol{D}^{i+1})) = \mathsf{Pr}(\mathrm{gtt}(\boldsymbol{D}^i))\mathsf{Pr}(\mathrm{gtt}(\boldsymbol{D}^{i+1}))$$
$$\mathsf{Pr}(\mathrm{gtt}(\boldsymbol{D}^i) \wedge \mathrm{gtf}(\boldsymbol{D}^{i+1})) = \mathsf{Pr}(\mathrm{gtt}(\boldsymbol{D}^i))\mathsf{Pr}(\mathrm{gtf}(\boldsymbol{D}^{i+1}))$$
$$\mathsf{Pr}(\mathrm{gtf}(\boldsymbol{D}^i) \wedge \mathrm{gtt}(\boldsymbol{D}^{i+1})) = \mathsf{Pr}(\mathrm{gtf}(\boldsymbol{D}^i))\mathsf{Pr}(\mathrm{gtt}(\boldsymbol{D}^{i+1}))$$
$$\mathsf{Pr}(\mathrm{gtf}(\boldsymbol{D}^i) \wedge \mathrm{gtf}(\boldsymbol{D}^{i+1})) = \mathsf{Pr}(\mathrm{gtf}(\boldsymbol{D}^i))\mathsf{Pr}(\mathrm{gtf}(\boldsymbol{D}^{i+1}))$$

F. Logical Tautologies for Detectors

All of the tautologies in this subsection are straightforwardly derived from the semantics of the operators by calculating and comparing the events on both sides.

These tautologies belong to two rule lists: $\mathcal{R}_{\mathrm{log}}$ and $\mathcal{R}_{\mathrm{ev}}$. Both lists are used in Step 1 of the analysis part. The rules replace the left part with the right part of the equations

Multiple Negations: Double negations can be removed with $\neg_s$, but not with $\neg_w$ or $\neg_{se}$:

$$\neg_s\neg_s\boldsymbol{D} = \boldsymbol{D} \qquad (\mathcal{R}_{\mathrm{log}})$$
$$\neg_w\neg_w\boldsymbol{D} \neq \boldsymbol{D}$$
$$\neg_{se}\neg_{se}\boldsymbol{D} \neq \boldsymbol{D}$$

However, limited tautologies apply to double negations of $\neg_w$ and $\neg_{se}$:

$$\mathrm{dot}(\neg_w\neg_w\boldsymbol{D}) = \mathrm{dot}(\boldsymbol{D}) \qquad (\mathcal{R}_{\mathrm{ev}})$$
$$\mathrm{gtt}(\neg_w\neg_w\boldsymbol{D}) = \mathrm{gtt}(\boldsymbol{D}) \qquad (\mathcal{R}_{\mathrm{ev}})$$
$$\mathrm{gtf}(\neg_w\neg_w\boldsymbol{D}) = \mathrm{gtf}(\boldsymbol{D}) \qquad (\mathcal{R}_{\mathrm{ev}})$$
$$\mathrm{dof}(\neg_{se}\neg_{se}\boldsymbol{D}) = \mathrm{dof}(\boldsymbol{D}) \qquad (\mathcal{R}_{\mathrm{ev}})$$
$$\mathrm{gtt}(\neg_{se}\neg_{se}\boldsymbol{D}) = \mathrm{gtt}(\boldsymbol{D}) \qquad (\mathcal{R}_{\mathrm{ev}})$$
$$\mathrm{gtf}(\neg_{se}\neg_{se}\boldsymbol{D}) = \mathrm{gtf}(\boldsymbol{D}) \qquad (\mathcal{R}_{\mathrm{ev}})$$

Any triple negation reduces to a single negation:

$$\neg_w\neg_w\neg_w\boldsymbol{D} = \neg_w\boldsymbol{D} \qquad (\mathcal{R}_{\mathrm{log}}) \qquad (10)$$
$$\neg_{se}\neg_{se}\neg_{se}\boldsymbol{D} = \neg_{se}\boldsymbol{D} \qquad (\mathcal{R}_{\mathrm{log}}) \qquad (11)$$

Different negations are not commutative, but $\neg_w$ and $\neg_{se}$ "switch" when $\neg_s$ passes over them and the negation outside $\neg_w$ and $\neg_{se}$ can be replaced with any other negation:

$$\neg_s\neg_w\boldsymbol{D} \neq \neg_w\neg_s\boldsymbol{D}$$
$$\neg_s\neg_{se}\boldsymbol{D} \neq \neg_{se}\neg_s\boldsymbol{D}$$
$$\neg_w\neg_{se}\boldsymbol{D} \neq \neg_{se}\neg_w\boldsymbol{D}$$

$$\neg_s\neg_w\boldsymbol{D} = \neg_{se}\neg_s\boldsymbol{D} = \neg_{se}\neg_w\boldsymbol{D} = \neg_w\neg_w\boldsymbol{D} \ (\mathcal{R}_{\mathrm{log}}) \quad (12)$$
$$\neg_s\neg_{se}\boldsymbol{D} = \neg_w\neg_s\boldsymbol{D} = \neg_w\neg_{se}\boldsymbol{D} = \neg_{se}\neg_{se}\boldsymbol{D} \ (\mathcal{R}_{\mathrm{log}})$$

De Morgan's and Distribution Laws: De Morgan's laws apply to $\neg_s$:

$$\neg_s(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b) = \neg_s\boldsymbol{D}_a \boldsymbol{\wedge} \neg_s\boldsymbol{D}_b \qquad (\mathcal{R}_{\mathrm{log}}) \qquad (13)$$
$$\neg_s(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b) = \neg_s\boldsymbol{D}_a \boldsymbol{\vee} \neg_s\boldsymbol{D}_b \qquad (\mathcal{R}_{\mathrm{log}}) \qquad (14)$$

For $\neg_w$ and $\neg_{se}$, De Morgan's laws work for disjunction and conjunction respectively, but not the other way around:

$$\neg_w(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b) = \neg_w\boldsymbol{D}_a \boldsymbol{\wedge} \neg_w\boldsymbol{D}_b \qquad (\mathcal{R}_{\mathrm{log}})$$
$$\neg_{se}(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b) = \neg_{se}\boldsymbol{D}_a \boldsymbol{\vee} \neg_w\boldsymbol{D}_b \qquad (\mathcal{R}_{\mathrm{log}})$$

$$\neg_w(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b) \neq \neg_w\boldsymbol{D}_a \boldsymbol{\vee} \neg_w\boldsymbol{D}_b$$
$$\neg_{se}(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b) \neq \neg_{se}\boldsymbol{D}_a \boldsymbol{\wedge} \neg_{se}\boldsymbol{D}_b$$

But limited tautologies are available for the other two cases:

$$\begin{aligned}\mathrm{dof}(\neg_w(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b)) &= \mathrm{dof}(\neg_w\boldsymbol{D}_a \boldsymbol{\vee} \neg_w\boldsymbol{D}_b)\\ &= \mathrm{dot}(\boldsymbol{D}_a) \wedge \mathrm{dot}(\boldsymbol{D}_b) \qquad (\mathcal{R}_{\mathrm{ev}})\end{aligned}$$
$$\begin{aligned}\mathrm{dot}(\neg_{se}(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b)) &= \mathrm{dot}(\neg_{se}\boldsymbol{D}_a \boldsymbol{\wedge} \neg_{se}\boldsymbol{D}_b)\\ &= \mathrm{dof}(\boldsymbol{D}_a) \wedge \mathrm{dof}(\boldsymbol{D}_b) \qquad (\mathcal{R}_{\mathrm{ev}})\end{aligned}$$

Operators $\boldsymbol{\vee}$ and $\boldsymbol{\wedge}$ are distributive. Only distribution of conjunctions is used in simplification:

$$(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b) \boldsymbol{\wedge} \boldsymbol{D}_c = \boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_c \boldsymbol{\vee} \boldsymbol{D}_b \boldsymbol{\wedge} \boldsymbol{D}_c \quad (\mathcal{R}_{\mathrm{log}})$$
$$(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b) \boldsymbol{\vee} \boldsymbol{D}_c = (\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_c) \boldsymbol{\wedge} (\boldsymbol{D}_b \boldsymbol{\vee} \boldsymbol{D}_c)$$

Temporal Modalities: With temporal compositions, $\neg_s$ behaves like a binary negation with LTL modalities, whereas $\neg_w$ and $\neg_{se}$ only do for one of the modalities:

$$\neg_s\Box_{[m,n]}\boldsymbol{D} = \Diamond_{[m,n]}\neg_s\boldsymbol{D} \qquad (\mathcal{R}_{\mathrm{log}})$$
$$\neg_s\Diamond_{[m,n]}\boldsymbol{D} = \Box_{[m,n]}\neg_s\boldsymbol{D} \qquad (\mathcal{R}_{\mathrm{log}}) \qquad (15)$$
$$\neg_w\Diamond_{[m,n]}\boldsymbol{D} = \Box_{[m,n]}\neg_w\boldsymbol{D} \qquad (\mathcal{R}_{\mathrm{log}})$$
$$\neg_{se}\Box_{[m,n]}\boldsymbol{D} = \Diamond_{[m,n]}\neg_{se}\boldsymbol{D} \qquad (\mathcal{R}_{\mathrm{log}})$$

$$\neg_w\Box_{[m,n]}\boldsymbol{D} \neq \Diamond_{[m,n]}\neg_w\boldsymbol{D}$$
$$\neg_{se}\Diamond_{[m,n]}\boldsymbol{D} \neq \Box_{[m,n]}\neg_{se}\boldsymbol{D}$$

Error Rates: Negations $\boldsymbol{\neg}_w$ and $\boldsymbol{\neg}_{se}$ are better-behaved when it comes to calculating error rates: unlike $\boldsymbol{\neg}_s$, they do not introduce the dependency on the probability of detector non-confidence:

$$\begin{aligned}
\mathrm{fpr}(\boldsymbol{\neg}_s \boldsymbol{D}) &= \mathrm{fnr}(\boldsymbol{D}) - \mathrm{Pr}(\mathrm{dou}(\boldsymbol{D}) \mid \mathrm{gtt}(\boldsymbol{D})) && (\mathcal{R}_{\text{log}})\\
\mathrm{fnr}(\boldsymbol{\neg}_s \boldsymbol{D}) &= \mathrm{fpr}(\boldsymbol{D}) + \mathrm{Pr}(\mathrm{dou}(\boldsymbol{D}) \mid \mathrm{gtf}(\boldsymbol{D})) && (\mathcal{R}_{\text{log}})\\
\mathrm{fpr}(\boldsymbol{\neg}_w \boldsymbol{D}) &= \mathrm{fpr}(\boldsymbol{\neg}_{se} \boldsymbol{D}) = \mathrm{fnr}(\boldsymbol{D}) && (\mathcal{R}_{\text{log}})\\
\mathrm{fnr}(\boldsymbol{\neg}_w \boldsymbol{D}) &= \mathrm{fnr}(\boldsymbol{\neg}_{se} \boldsymbol{D}) = \mathrm{fpr}(\boldsymbol{D}) && (\mathcal{R}_{\text{log}})
\end{aligned}$$

For fully independent detectors $\boldsymbol{D}_a$ and $\boldsymbol{D}_b$ (i.e., any pair of events from two detectors is conditionally and unconditionally independent), these rate formulas apply:

$$\begin{aligned}
\mathrm{fpr}(\boldsymbol{D}_a \boldsymbol{\vee} \boldsymbol{D}_b) &= 1 - (1 - \mathrm{fpr}(\boldsymbol{D}_a))(1 - \mathrm{fpr}(\boldsymbol{D}_b))\\
\mathrm{fnr}(\boldsymbol{D}_a \boldsymbol{\wedge} \boldsymbol{D}_b) &= 1 - (1 - \mathrm{fnr}(\boldsymbol{D}_a))(1 - \mathrm{fnr}(\boldsymbol{D}_b))
\end{aligned}$$

G. Rules for Probability Reasoning

Below is a full list of rules, denoted $\mathcal{R}_{\text{prob}}$, that can be used for manipulating probability formulas. First are the parameter-free rules over any expressions A, B, and C. Symbols dnf and cnf are the functions that return the disjunctive and conjunctive normal forms of input event expressions, respectively:

$$\begin{aligned}
\mathsf{Pr}(\mathsf{T}) &\rightarrow 1\\
\mathsf{Pr}(\mathsf{F}) &\rightarrow 0\\
\mathsf{Pr}(A \mid \mathsf{T}) &\rightarrow \mathsf{Pr}(A)\\
\mathsf{Pr}(\neg A) &\rightarrow 1 - \mathsf{Pr}(A)\\
\mathsf{Pr}(A) &\rightarrow 1 - \mathsf{Pr}(\neg A)\\
\mathsf{Pr}(\neg A \mid B) &\rightarrow 1 - \mathsf{Pr}(A \mid B) && (16)\\
\mathsf{Pr}(A \mid B) &\rightarrow 1 - \mathsf{Pr}(\neg A \mid B) && (17)\\
\mathsf{Pr}(A \mid B) &\rightarrow \mathsf{Pr}(A \wedge B)/\mathsf{Pr}(B)\\
\mathsf{Pr}(A \wedge B) &\rightarrow \mathsf{Pr}(A \mid B)\,\mathsf{Pr}(B)\\
\mathsf{Pr}(A \vee B) &\rightarrow \mathsf{Pr}(A) + \mathsf{Pr}(B) - \mathsf{Pr}(A \wedge B)\\
\mathsf{Pr}(A \vee B \mid C) &\rightarrow \mathsf{Pr}(A \mid C) + \mathsf{Pr}(B \mid C)\\
&\qquad - \mathsf{Pr}(A \wedge B \mid C) && (18)\\
\mathsf{Pr}(A \wedge B \mid C) &\rightarrow \mathsf{Pr}(A \mid B \wedge C)\,\mathsf{Pr}(B \mid C)\\
\mathsf{Pr}(A \mid B) &\rightarrow \mathsf{Pr}(B \mid A)\,\mathsf{Pr}(A)/\mathsf{Pr}(B)\\
\mathsf{Pr}(A) &\rightarrow \mathsf{Pr}(\mathrm{dnf}(A))\\
\mathsf{Pr}(A \mid B) &\rightarrow \mathsf{Pr}(\mathrm{dnf}(A) \mid B)\\
\mathsf{Pr}(A) &\rightarrow \mathsf{Pr}(\mathrm{cnf}(A))\\
\mathsf{Pr}(A \mid B) &\rightarrow \mathsf{Pr}(\mathrm{cnf}(A) \mid B) && (19)\\
[A \perp\!\!\!\perp C \mid B]\ \mathsf{Pr}(A \mid B \wedge C) &\rightarrow \mathsf{Pr}(A \mid B) && (20)\\
[A \perp\!\!\!\perp B \mid C]\ \mathsf{Pr}(A \wedge B \mid C) &\rightarrow \mathsf{Pr}(A \mid C)\,\mathsf{Pr}(B \mid C)\\
& && (21)
\end{aligned}$$

Parametric rules for probability manipulation, also part of $\mathcal{R}_{\text{prob}}$, use any event expression X to produce new formulas:

$$\begin{aligned}
\mathsf{Pr}(A) &\rightarrow \mathsf{Pr}(A \wedge X)/\mathsf{Pr}(X \mid A)\\
\mathsf{Pr}(A \mid B) &\rightarrow \mathsf{Pr}(A \wedge X \mid B)/\mathsf{Pr}(X \mid A \wedge B)\\
\mathsf{Pr}(A) &\rightarrow \mathsf{Pr}(A \wedge X) + \mathsf{Pr}(A \wedge \neg X)\\
\mathsf{Pr}(A \mid B) &\rightarrow \mathsf{Pr}(A \wedge X \mid B) + \mathsf{Pr}(A \wedge \neg X \mid B)
\end{aligned}$$

Finally, $\mathcal{R}_{\text{prob}}$ has the capacity to equivalently replace marginal events:

$$\begin{aligned}
\mathrm{dot}(\boldsymbol{D}) &\rightarrow \neg\,\mathrm{dof}(\boldsymbol{D}) \wedge \neg\,\mathrm{dou}(\boldsymbol{D}) && (22)\\
\mathrm{dof}(\boldsymbol{D}) &\rightarrow \neg\,\mathrm{dot}(\boldsymbol{D}) \wedge \neg\,\mathrm{dou}(\boldsymbol{D}) && (23)\\
\mathrm{dou}(\boldsymbol{D}) &\rightarrow \neg\,\mathrm{dot}(\boldsymbol{D}) \wedge \neg\,\mathrm{dof}(\boldsymbol{D})\\
\mathrm{gtt}(\boldsymbol{D}) &\rightarrow \neg\,\mathrm{gtf}(\boldsymbol{D})\\
\mathrm{gtf}(\boldsymbol{D}) &\rightarrow \neg\,\mathrm{gtt}(\boldsymbol{D})
\end{aligned}$$

H. Rules for Independence Reasoning

The list $\mathcal{R}_{\text{indep}}$ contains rules for independence reasoning. Most of them are parameter-free independence rules for events A, B, C, and D (binary) with probability greater than 0:

$$\begin{gathered}
A \perp\!\!\!\perp B \rightarrow B \perp\!\!\!\perp A\\
A \perp\!\!\!\perp \neg B \rightarrow A \perp\!\!\!\perp B\\
A \perp\!\!\!\perp B \mid \mathsf{T} \rightarrow A \perp\!\!\!\perp B\\
A \perp\!\!\!\perp B \mid C \rightarrow B \perp\!\!\!\perp A \mid C\\
A \perp\!\!\!\perp \neg B \mid C \rightarrow A \perp\!\!\!\perp B \mid C\\
(A \perp\!\!\!\perp C \mid B) \wedge (A \perp\!\!\!\perp B) \rightarrow A \perp\!\!\!\perp B \wedge C\\
(A \perp\!\!\!\perp C \mid B \wedge D) \wedge (A \perp\!\!\!\perp B \mid D) \rightarrow A \perp\!\!\!\perp B \wedge C \mid D\\
(A \perp\!\!\!\perp C \mid B \wedge D) \wedge (A \perp\!\!\!\perp D \mid B) \rightarrow A \perp\!\!\!\perp D \wedge C \mid B\\
(A \perp\!\!\!\perp B \wedge C) \rightarrow (A \perp\!\!\!\perp B)\ \wedge (A \perp\!\!\!\perp C \mid B)\\
(A \perp\!\!\!\perp B \wedge C) \rightarrow (A \perp\!\!\!\perp C)\ \wedge (A \perp\!\!\!\perp B \mid C)\\
(A \perp\!\!\!\perp B \wedge C \mid D) \rightarrow (A \perp\!\!\!\perp C \mid D)\ \wedge (A \perp\!\!\!\perp B \mid C \wedge D)\\
(A \perp\!\!\!\perp B \mid C) \wedge (A \perp\!\!\!\perp C \mid B) \rightarrow (A \perp\!\!\!\perp B \wedge C)\\
(A \perp\!\!\!\perp B \mid C \wedge D) \wedge (A \perp\!\!\!\perp C \mid B \wedge D) \rightarrow (A \perp\!\!\!\perp B \wedge C \mid D)\\
(A \perp\!\!\!\perp B \mid C \wedge D) \wedge (A \perp\!\!\!\perp D \mid B \wedge C) \rightarrow (A \perp\!\!\!\perp B \wedge D \mid C)
\end{gathered}$$

A single parametric independence rule used is for any expression X with probability greater than 0:

$$(A \perp\!\!\!\perp B \mid C) \wedge (A \perp\!\!\!\perp X \mid B \wedge C) \rightarrow (A \perp\!\!\!\perp X \mid C)$$

I. Full Derivation of Error Rate Formulas for Monitors

FNR for Monitor of Pipeline Recovery: Here we illustrate the Steps 1–3 for the NCC/ECC analysis of the FNR of $\boldsymbol{M}_{pr}$. Suppose that the ECC's known probabilities and the NCC's preferred probabilities are the same and equal $\{\mathrm{fnr}(\boldsymbol{Pl})\}$. The independence assumptions are found in Equations (4) and (6) in the main paper.

The analysis uses the following rules $\mathcal{R}$:

- $\mathcal{R}_{\text{log}}$: Equations 1, 13, 15, 12, 10, and 8.
- $\mathcal{R}_{\text{ev}}$: Equations 6, 7, 4, 5, 2, and 3.
- $\mathcal{R}_{\text{prob}}$: 16, 21, 20, 17, 23, 19, 18, 22.
- $\mathcal{R}_{\text{indep}} = \emptyset$ (none are needed because the assumption matches the events exactly).

The monitor is described by the following property:

$$\boldsymbol{M}_{pr} = \boldsymbol{\neg}_s(\boldsymbol{\neg}_w \boldsymbol{Pl} \boldsymbol{\rightarrow}_w \boldsymbol{\Diamond}_{[1,d]} \boldsymbol{Pl})$$

The analysis of $\mathrm{fnr}(\boldsymbol{M}_{pr})$ starts with Step 1.1. It uses the rule in Equation (1) to rewrite $\boldsymbol{\rightarrow}_w$ with $\boldsymbol{\neg}_w$:

$$\boldsymbol{\neg}_s(\boldsymbol{\neg}_w \boldsymbol{Pl} \boldsymbol{\rightarrow}_w \boldsymbol{\Diamond}_{[1,d]} \boldsymbol{Pl}) = \boldsymbol{\neg}_s(\boldsymbol{\neg}_w \boldsymbol{\neg}_w \boldsymbol{Pl} \boldsymbol{\vee} \boldsymbol{\Diamond}_{[1,d]} \boldsymbol{Pl})$$

Next, Step 1.1 advances $\boldsymbol{\neg}_s$ using Equations (15) and (13):

$$\boldsymbol{\neg}_s(\boldsymbol{\neg}_w\boldsymbol{\neg}_w\boldsymbol{Pl} \boldsymbol{\vee} \boldsymbol{\Diamond}_{[1,d]}\boldsymbol{Pl}) = \boldsymbol{\neg}_s\boldsymbol{\neg}_w\boldsymbol{\neg}_w\boldsymbol{Pl} \boldsymbol{\wedge} \boldsymbol{\Box}_{[1,d]}\boldsymbol{\neg}_s\boldsymbol{Pl}$$

Step 1.1 replaces $\boldsymbol{\neg}_s\boldsymbol{\neg}_w\boldsymbol{\neg}_w\boldsymbol{Pl}$ with $\boldsymbol{\neg}_w\boldsymbol{\neg}_w\boldsymbol{\neg}_w\boldsymbol{Pl}$ using Equation (12) (refer to the first and last expressions), and $\boldsymbol{\neg}_w\boldsymbol{\neg}_w\boldsymbol{\neg}_w\boldsymbol{Pl}$ with $\boldsymbol{\neg}_w\boldsymbol{Pl}$ using Equation (10). Having done this, Step 1.1 has arrived at the following formula:

$$\mathrm{fnr}(\boldsymbol{\neg}_w\boldsymbol{Pl} \boldsymbol{\wedge} \boldsymbol{\Box}_{[1,d]}\boldsymbol{\neg}_s\boldsymbol{Pl})$$

Finally Equation (8), Step 1.1 rewrites $\boldsymbol{\Box}$ using a sequence of $\boldsymbol{\wedge}$ operators and outputs the following formula:

$$\mathrm{fnr}\left(\boldsymbol{\neg}_w\boldsymbol{Pl} \boldsymbol{\wedge} \boldsymbol{\neg}_s\boldsymbol{Pl}^1 \boldsymbol{\wedge} \ldots \boldsymbol{\wedge} \boldsymbol{\neg}_s\boldsymbol{Pl}^d\right)$$

Now, Step 1.2 replaces the fnr operator according to its definition: $\mathrm{fnr}(\boldsymbol{M}_{pr}) = \mathsf{Pr}(\neg\,\mathrm{dot}(\boldsymbol{M}_{pr}) \mid \mathrm{gtt}(\boldsymbol{M}_{pr})$. The events dot and dou of the composite detector above are replaced with Boolean combinations of events of atomic detectors, based on the rule for operators $\boldsymbol{\wedge}$, $\boldsymbol{\neg}_w$, and $\boldsymbol{\neg}_s$ in Equations (2) to (7):

$$\begin{aligned}\mathrm{dot}(\boldsymbol{M}_{pr}) =&\ (\mathrm{dof}(\boldsymbol{Pl}^0) \vee \mathrm{dou}(\boldsymbol{Pl}^0)) \wedge \mathrm{dof}(\boldsymbol{Pl}^1) \wedge \ldots\\ &\wedge \mathrm{dof}(\boldsymbol{Pl}^d)\\ \mathrm{gtt}(\boldsymbol{M}_{pr}) =&\ \mathrm{gtf}(\boldsymbol{Pl}^0) \wedge \mathrm{gtf}(\boldsymbol{Pl}^1) \wedge \ldots \wedge \mathrm{gtf}(\boldsymbol{Pl}^d)\end{aligned}$$

With all detector operators removed, Step 1.2 returns:

$$\begin{aligned}&\mathsf{Pr}(\neg((\mathrm{dof}(\boldsymbol{Pl}^0) \vee \mathrm{dou}(\boldsymbol{Pl}^0)) \wedge \mathrm{dof}(\boldsymbol{Pl}^1) \wedge \ldots\\ &\quad\wedge \mathrm{dof}(\boldsymbol{Pl}^d)) \mid \mathrm{gtf}(\boldsymbol{Pl}^0) \wedge \ldots \wedge \mathrm{gtf}(\boldsymbol{Pl}^d))\end{aligned}$$

Step 1.3 removes the negation using Equation (16):

$$\begin{aligned}&\mathsf{Pr}(\neg((\mathrm{dof}(\boldsymbol{Pl}^0) \vee \mathrm{dou}(\boldsymbol{Pl}^0)) \wedge \mathrm{dof}(\boldsymbol{Pl}^1) \wedge \ldots\\ &\quad\wedge \mathrm{dof}(\boldsymbol{Pl}^d)) \,|\mathrm{gtf}(\boldsymbol{Pl}^0) \wedge \ldots \wedge \mathrm{gtf}(\boldsymbol{Pl}^d)) =\\ &1 - \mathsf{Pr}(((\mathrm{dof}(\boldsymbol{Pl}^0) \vee \mathrm{dou}(\boldsymbol{Pl}^0)) \wedge \mathrm{dof}(\boldsymbol{Pl}^1) \wedge \ldots\\ &\quad\wedge \mathrm{dof}(\boldsymbol{Pl}^d)) \mid \mathrm{gtf}(\boldsymbol{Pl}^0) \wedge \ldots \wedge \mathrm{gtf}(\boldsymbol{Pl}^d))\end{aligned}$$

Now, Step 2.1 invokes the conditional independence rule in Equation (21) and launches Step 3 with the events under the probability in the equation above. Step 3.1 matches the events to the conditional independence of pipeline detections (DO^i) given the ground-truth of pipeline presence (GT^I) as stated in Equation (4) in the main paper.

Step 3.2 returns T to Step 2.1, and the rule in Equation (21) splits the probability into a product of individual detector events conditioned on the dof events of all detectors. Next, Equation (20) removes the conditioning from these probabilities by calling Step 3 and getting T due to Equation (6) in the main paper. This reduces the expression to the single-detector probability Pr:

$$\begin{aligned}&1 - \big(\mathrm{Pr}(\mathrm{dof}(\boldsymbol{Pl}) \vee \mathrm{dou}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl})\big)\times\\ &\qquad(\mathrm{Pr}(\mathrm{dof}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl}))^d\end{aligned}$$

Step 2.1 reintroduces the negation using Equation (17) and replaces the dof events with in accordance with Equation (23):

$$\begin{aligned}&1 - \big(1 - \mathrm{Pr}(\neg(\neg\,\mathrm{dot}(\boldsymbol{Pl}) \wedge \neg\,\mathrm{dou}(\boldsymbol{Pl}) \vee \mathrm{dou}(\boldsymbol{Pl})) \mid\\ &\mathrm{gtf}(\boldsymbol{Pl})\big)(1 - \mathrm{Pr}(\neg(\neg\,\mathrm{dot}(\boldsymbol{Pl}) \wedge \neg\,\mathrm{dou}(\boldsymbol{Pl})) \mid \mathrm{gtf}(\boldsymbol{Pl}))^d\end{aligned}$$

Now Step 2.1 uses the rule to put events into a CNF from Equation (19):

$$\begin{aligned}&1 - \big(1 - \mathrm{Pr}(\mathrm{dot}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl})\big)\times\\ &\qquad(1 - \mathrm{Pr}(\mathrm{dot}(\boldsymbol{Pl}) \vee \mathrm{dou}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl}))^d\end{aligned}$$

Next, Step 2.1 uses the rule from Equation (18) to break up the disjunction:

$$\begin{aligned}&1 - \big(1 - \mathrm{Pr}(\mathrm{dot}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl})\big)\times\\ &\quad(1 - \mathrm{Pr}(\mathrm{dot}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl})) - \mathrm{Pr}(\mathrm{dou}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl}))+\\ &\quad\mathrm{Pr}(\mathrm{dot}(\boldsymbol{Pl}) \wedge \mathrm{dou}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl})))^d\end{aligned}$$

The probabilities $\mathrm{Pr}(\mathrm{dot}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl}))$ are equivalent to $\mathrm{fpr}(\boldsymbol{Pl})$. Therefore, they are preferred and will not be affected by matching transformations.

Next, Step 2.1 executes a replacement of dot with the rule in Equation (22). This transforms $\mathrm{Pr}(\mathrm{dot}(\boldsymbol{Pl}) \wedge \mathrm{dou}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl})$ into $\mathrm{Pr}(\neg\,\mathrm{dof}(\boldsymbol{Pl}) \wedge \neg\,\mathrm{dou}(\boldsymbol{Pl}) \wedge \mathrm{dou}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl})$, which is replaced by 0 because of the contradiction: $\neg\,\mathrm{dou} \wedge \mathrm{dou}(\boldsymbol{Pl})$ (which is processed automatically by Mathematica). Step 2.1 finishes its rules with the following formula:

$$\begin{aligned}&1 - \big(1 - \mathrm{Pr}(\mathrm{dot}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl})\big)\times\\ &\quad(1 - \mathrm{Pr}(\mathrm{dot}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl})) - \mathrm{Pr}(\mathrm{dou}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl})))^d\end{aligned}$$

The above formula formula can be compactly rewritten into the final formula:

$$\begin{aligned}\mathrm{fnr}(\boldsymbol{M}_{pr}) =&1 - (1 - \mathrm{fpr}(\boldsymbol{Pl}))\Big(1 - \mathrm{fpr}(\boldsymbol{Pl}) -\\ &\qquad\mathrm{Pr}(\mathrm{dou}(\boldsymbol{Pl}) \mid \mathrm{gtf}(\boldsymbol{Pl}))\Big)^d \qquad (24)\end{aligned}$$

FPR for Monitor of Reliable Following: Here we briefly retrace Steps 1–3 of NCC/ECC for the FPR of monitor $\boldsymbol{M}_{rf}$, which alarms iff the following property is violated:

$$\boldsymbol{M}_{rf} = \boldsymbol{\neg}_s\boldsymbol{\Box}_{[0,d]}\boldsymbol{Pl}$$

The derivation of this FPR proceeds as follows. First, we advance the negation according to the tautologies above:

$$\boldsymbol{\Diamond}_{[0,d]}\boldsymbol{\neg}_s\boldsymbol{Pl}$$

Next, we write down the relevant events of the above detector:

$$\begin{aligned}\mathrm{dot}(\boldsymbol{M}_{rf}) &= \mathrm{dof}(\boldsymbol{Pl}^0) \vee \mathrm{dof}(\boldsymbol{Pl}^1) \vee \ldots \vee \mathrm{dof}(\boldsymbol{Pl}^d)\\ \mathrm{gtf}(\boldsymbol{M}_{rf}) &= \mathrm{gtt}(\boldsymbol{Pl}^0) \wedge \ldots \wedge \mathrm{gtt}(\boldsymbol{Pl}^d)\end{aligned}$$

Hence:

$$\begin{aligned}&\mathrm{fpr}(\boldsymbol{M}_{rf}) = \mathrm{Pr}(\mathrm{dof}(\boldsymbol{Pl}^0) \vee \mathrm{dof}(\boldsymbol{Pl}^1) \vee \ldots \vee \mathrm{dof}(\boldsymbol{Pl}^d) \mid\\ &\quad\mathrm{gtt}(\boldsymbol{Pl}^0) \wedge \ldots \wedge \mathrm{gtt}(\boldsymbol{Pl}^d)) =\\ &1 - \mathrm{Pr}(\neg\,\mathrm{dof}(\boldsymbol{Pl}^0) \wedge \neg\,\mathrm{dof}(\boldsymbol{Pl}^1) \wedge \ldots \wedge \neg\,\mathrm{dof}(\boldsymbol{Pl}^d) \mid\\ &\qquad\mathrm{gtt}(\boldsymbol{Pl}^0) \wedge \ldots \wedge \mathrm{gtt}(\boldsymbol{Pl}^d))\end{aligned}$$

Now, assuming the conditional independence of pipeline detections (DO^i) given the ground-truth of pipeline presence (GT^i) as stated in Equation (4) in the main paper, the above expression simplifies to a final formula for $\boldsymbol{M}_{rf}$:

$$\mathrm{fpr}(\boldsymbol{M}_{rf}) = 1 - \Big(1 - \mathrm{fnr}(\boldsymbol{Pl}) + \mathrm{Pr}(\mathrm{dou}(\boldsymbol{Pl}) \mid \mathrm{gtt}(\boldsymbol{Pl}))\Big)^{d+1}$$

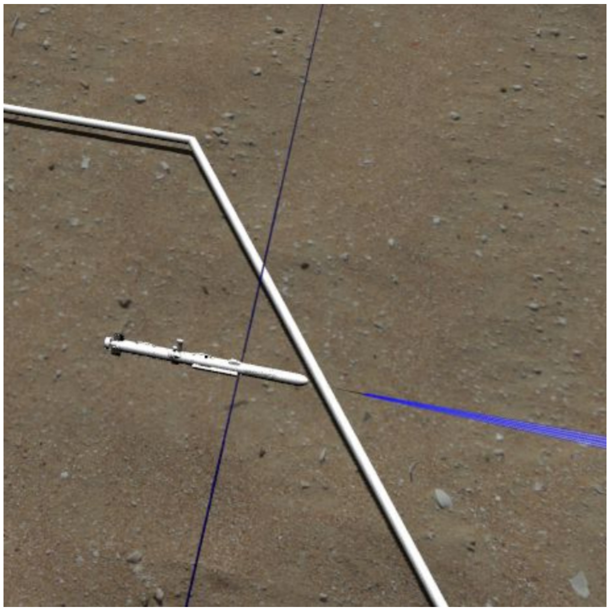

Figure 1: A UUV moves to the right above a pipeline. The blue beam shows the obstacle detection sonar, and a plane perpendicular to the figure shows the seafloor-facing scans of the side-looking sonars.

J. Additional Figures for Evaluation

This section contains several auxiliary figures:

- Figure 1 shows a screenshot from our UUV simulator.
- Figure 2 shows the estimates of the FNR of M_{pr} for different values of deadline d, based on our full dataset.
- Figure 3 shows the estimates of the FPR of $\boldsymbol{M_{rf}}$ for different values of deadline d, based on our full dataset.
- As Figure 4 indicates for $\boldsymbol{M_{pr}}$ ($d = 10$), BBC converges to the ground truth as the amount of information in the dataset increases, whereas NCC converges as well, but in a biased manner. The bias is, however, contained for all d in a 95% Binomial confidence interval (CI) for ECC (a vertical line; based on the maximum x-value), indicating that it is likely to be an artifact of sampling randomness. A similar convergence pattern occurs for the other values of d with different convergence rates.
- Figure 5 is the same type as the previous figure, but for FPR of $\boldsymbol{M_{rf}}$. It shows similar yet unbiased convergence of NCC and BBC to ECC for $d = 10$ (other values of d repeat this pattern too).
- Figure 6 shows the same type of a plot as Figure 3 in the main paper, but for the FPR of $\boldsymbol{M_{rf}}$. Here, the x-axis bin width is 400, and the minimum number of points per bin is 38. We can see that the errors of NCC and BBC
- Figure 7 aggregates the information from plots like Figure 6 (and Figure 3 in the main paper) for *all* deadlines. We plot for each d the RMSE across all samples with varied information count. We observe that for larger decrease rapidly (note the logarithmic scale) for more data, and NCC errors are consistently smaller than those of BBC. Further analysis showed this difference grows with d, and the cross-over point shifts to the right.
deadlines, particularly in the case of $\boldsymbol{M_{pr}}$, the average error grows faster for BBC than for NCC.
- Figure 8 shows the dependency of the FPR estimates of $\boldsymbol{M_{rf}}$ (NCC, BBC) on the various levels of stateful noise (w). These estimates are made on our full dataset and for $d = 10$.

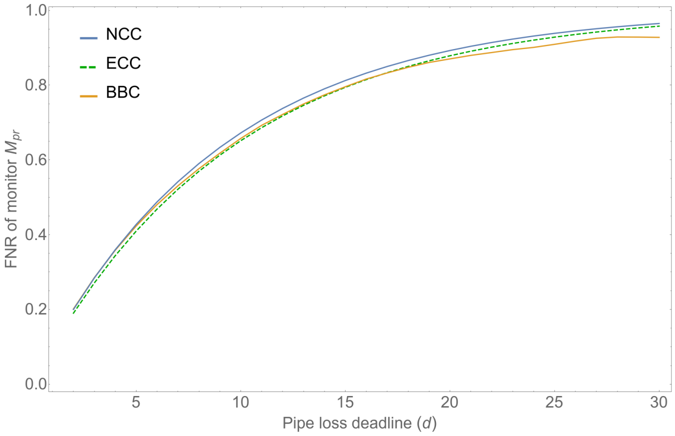

Figure 2: Full-data estimates of the FNR of M_{pr}. BBC is less accurate for $d > 25$.

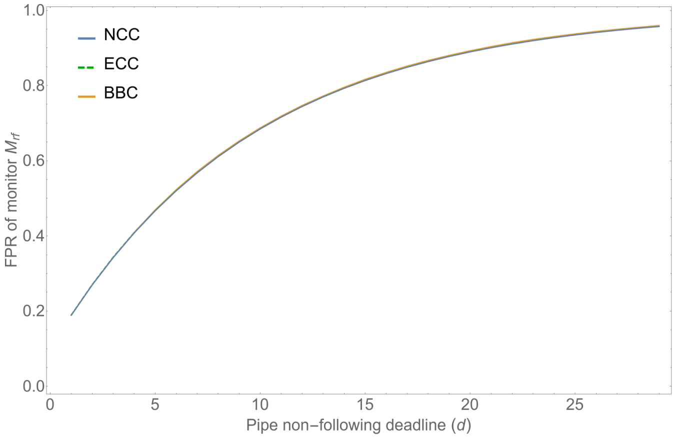

Figure 3: Full-data estimates of the FPR of $\boldsymbol{M_{rf}}$. The estimates are indistinguishably close.

References

[1] S. C. Kleene, *Introduction to metamathematics*. Amsterdam, The Netherlands: North-Holland Publishing Co, 1952.

[2] A. Pnueli, "The temporal logic of programs," in *18th Annual Symposium on Foundations of Computer Science, 1977*, Oct. 1977, pp. 46–57.

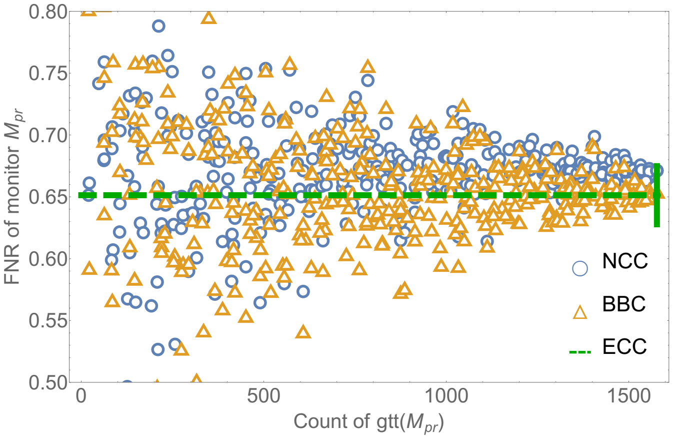

Figure 4: Estimates of FNR of M_{pr} ($d = 10$) by information count. The vertical ECC line is a 95% CI for max x-value.

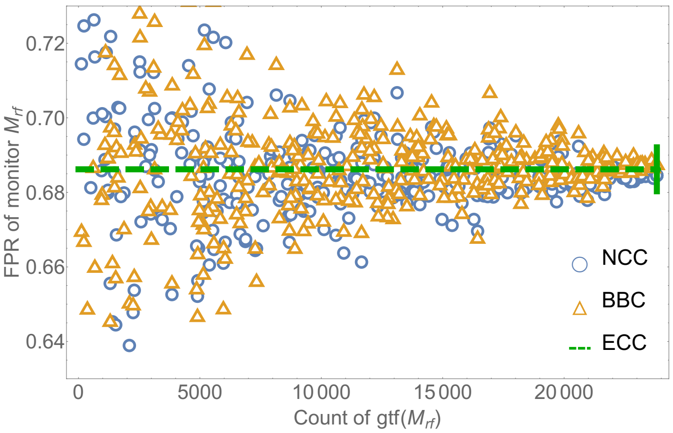

Figure 5: Estimates of FPR of M_{rf} ($d = 10$) by information count. The vertical ECC line is a 95% CI for max x-value.

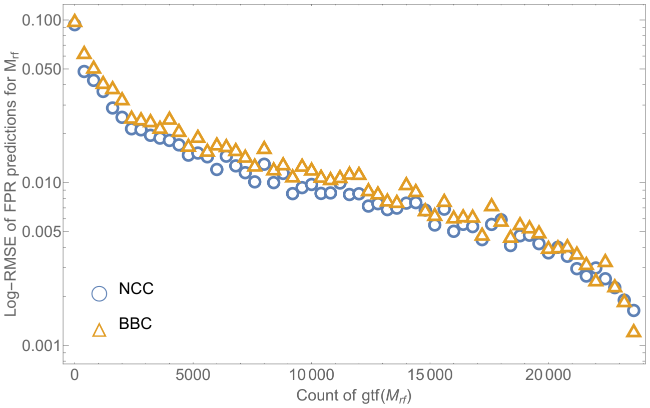

Figure 6: Log-RMSE of FPR estimates for M_{rf} ($d = 10$) by information count.

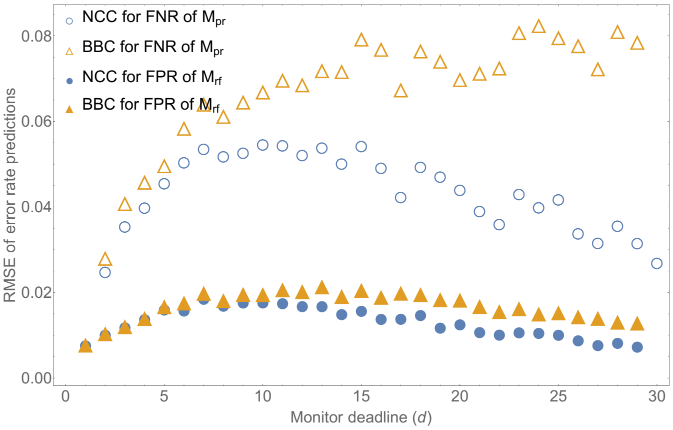

Figure 7: RMSE of NCC and BBC for M_{pr} (high) and M_{rf} (low), relative to the respective deadline d.

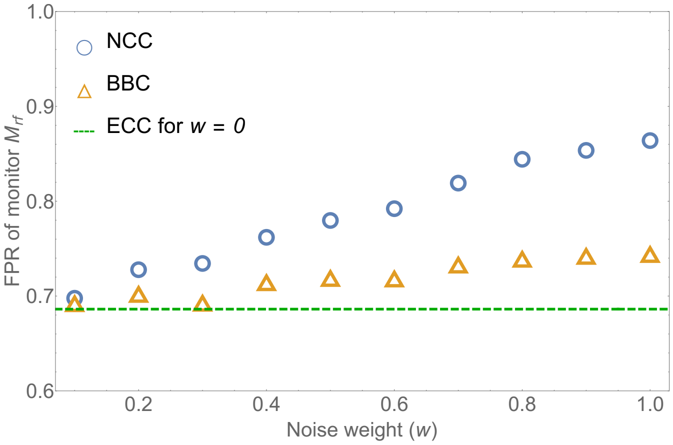

Figure 8: NCC and BBC for FPR of M_{rf} ($d = 10$) relative to weight w. Baseline ECC is shown for $w = 0$, for context.