

Monitor

1. The Scout should at some point in time send a harvesting position to the Collector.

- **LTL:** $F(\text{sendHarvest})$
- **Not Safety:** There is no bad prefix because for every infinite trace that is not in L we can always append $\{\text{sendHarvest}\}$. This would then be a good prefix. \emptyset^ω does not have a bad prefix
- **Co-Safety:** Every trace in L has sendHarvest at some point which is a good prefix.
- **Monitorable:** Every finite trace can be extended to a good prefix by appending $\{\text{sendHarvest}\}$ so we do not have an ugly prefix.
- **Automaton** Paste here.

2. The Collector should always check its proximity sensors unless it is at a decent harvesting position.

- **LTL:** $G(\neg \text{atHarvest} \implies \text{checkingProximity})$
- **Safety:** Every trace not in L has at least one prefix $\{\sim \text{atHarvest} \implies \neg \text{checkingProximity}\}$ which is a bad prefix.
- **Not Co-Safety:** $\{\text{atHarvest}, \text{checkProximity}\}^\omega$ does not have a good prefix. Every trace that is in L does not have a good prefix because we can always do $\{\neg \text{atHarvest} \wedge \neg \text{checkingProximity}\}$ in the next step.
- **Monitorable:** Every finite trace can be extended to a bad prefix so it does not have an ugly prefix.
- **Automaton** Paste here.

3. A robot should never ignore three consecutive PING messages.

- **LTL:** $G(((\neg \text{pong} \wedge \text{ping}) \implies X((\neg \text{pong} \wedge \text{ping}) \implies X((\sim \text{pong} \wedge \text{ping}) \implies X(\text{pong}))))))$
- **Safety:** Every trace not in L has at least one prefix x which is a bad prefix.
- **Not Co-Safety:** $\{\text{pong}\}^\omega$ does not have a good prefix. We can extend every good trace to a bad trace by appending $\{\text{ping}, \text{ping}, \text{ping}, \text{ping}\}$.
- **Monitorable:** Every finite trace can be extended with the finite trace $\{\text{ping}, \text{ping}, \text{ping}, \text{ping}\}$ to a bad prefix, therefore we do not have an ugly prefix.
- **Automaton** Paste here.

4. When receiving a message, the robot copies the data over into a buffer. This buffer should be emptied at least every 500ms.

- **LTL:** This specification cannot be expressed in LTL but only in TLTL.

Embedded Systems Milestone 1

- **Safety:** Every trace not in L has at least one prefix where the buffer is not emptied for more than 500ms, which is a bad prefix.
- **Not Co-Safety:** $\{(\text{emptyBuffer}, t)\}^\omega$ does not have a good prefix for all $t \in \mathbb{N}$. We can extend every such good trace to a bad trace by appending $\{(\text{emptyBuffer}, t + 501)\}$.
- **Monitorable:** Every finite trace be extended to a bad prefix, therefore we do not have an ugly prefix.
- **Automaton:** Not sure if this should be done?