Definition

Now we ask, "How could the system enter hazardous states?"

We focus on how actions taken by parts of the system could cause hazards, if those actions occur under inappropriate conditions. We use a table with these guides:

- Control action required for safety is not provided or not followed
- An unsafe control action is provided that leads to a hazard (action inappropriate)
- A potentially safe control action is provided too late, too early, or out of sequence (occurs at wrong time)
- A safe control action is stopped too soon or applied too long (occurs for wrong duration)

Each cell entry is marked with “not applicable”, “not hazardous”, or a description of the **context** that makes the action dangerous and the **hazard** that results.

Thermostat Example

Action	**not provided**	**provided (but wrong)**	**too late, too early, out of sequence**	**applied for wrong duration**
Turn heat ON	If the room temperature is too low, not turning the furnace (H2)	If the room is already too hot (H3), if the heater is already on (H4)	Too long after the tempera-ture has fallen below threshold (H2), Too soon after turning the heater off (H3)	N/A

Desired Qualities

- Completeness — Check each cell.
- Each cell entry is marked with “not applicable”, “not hazardous”, or a description of the **context** that makes the action dangerous and the **hazard** that results.
- It is acceptable for a cell to include multiple (context,hazard) pairs.

Strategic Approaches

- Divide and conquer — This work can be split up among several people.
- Pace your efforts — Track progress, returning later as needed.
- Triage and prioritize — This table can get huge. With limited time resources, we may choose not to aim for completeness.

  Prioritize investigating actions needing additional scrutiny, e.g. actions that are new, poorly understood, currently changing, believed to be risky, or involved in close interactions with other systems that need additional scrutiny.

Toolkit: Unsafe Control Actions table

Relationship to other concepts

The **actions** we are analyzing here come from our **control model**.

The judgement of whether an action occurring inappropriately (or inappropriately failing to occur) is a *problem* comes from associating it with a **hazard**, which we have identified as a precursor to at least one **loss**.