Observability

We have so far assumed that we can observe events.

It is also possible that it is not possible to observe all events, which can be due to

- Limitations of the sensors, cannot measure the event itself. Faults are often unobservable, e.g. a stuck valve may manifest itself later by too high or too low pressure.

- Long distance between parts of the system, communication too slow, too expensive, or too unreliable

Unobservability of some events will put additional constraints on a supervisor.
Definition of observability for supervisors

Let $K$ (typically $= \mathcal{L}(S/G)$) and $M = \overline{M}$ (typically $= \mathcal{L}(G)$) be languages over an event set $\Sigma$. Let $\Sigma_c$ (controllable events) and $\Sigma_o$ (observable events) be subsets of $\Sigma$. Let $P$ be the natural projection from $\Sigma^*$ to $\Sigma_o^*$.

$K$ is said to be observable with respect to $M$, $P$ (or $\Sigma_o$), and $\Sigma_c$ if for all $s \in K$ and for all $\sigma \in \Sigma_c$

$$(s\sigma \notin \overline{K}) \text{ and } (s\sigma \in M) \Rightarrow P^{-1}[P(s)]\sigma \cap \overline{K} = \emptyset$$

In words: If a string $s\sigma$ is forbidden by the supervisor (with the language $K$), all other strings that looks like $s\sigma$ should also be forbidden.

If you cannot differentiate between two strings, then these strings should require the same control action.

If you must disable an event after observing a string, then by doing so you should not disable any string that appears in the desired behavior.

Example 40. Let $\Sigma = \{u, b\}$ and consider the language $M = \overline{\{ub, bu\}}$.

Is the language $K_1 = \{bu\}$ observable with respect to $M$, $\Sigma_o = \{b\}$, and $\Sigma_c = \{u\}$?

Is $K_2 = \{ub\}$ observable with respect to $M$, $\Sigma_o = \{b\}$, and $\Sigma_c = \{b\}$?
Solution to Example 38

Test all strings that looks like a string in $\overline{K_1} = \{\varepsilon, b, bu\}$ for if a controllable event (only $u$ in this case) is forbidden by the supervisor but allowed by the plant. After $\varepsilon$, $u$ is disabled by the supervisor, and thus no strings that looks like $\varepsilon$ can take place ($u$). After $b$, $u$ is allowed by the plant and strings that look like $bu$ are forbidden by the plant. After $bu$ no strings are enabled by neither the plant nor the controller. So $K_1$ is observable.

For $K_2$ we analyze strings that looks like $\{\varepsilon, u, ub\}$. After $\varepsilon$ the supervisor should disable $b$. After $u$ the supervisor should enable $b$, but $u$ looks like $\varepsilon$ as $u$ is not observable. So the supervisor do not know if $b$ should be allowed initially, because we do not know whether $u$ has happened or not. So $K_2$ is not observable.

In the latter case we note that $u$ is neither controllable nor observable. As we have no contact to the event, it is trivially so that a supervisor can never rely on such events.
Nonblocking, controllable and observable

If we have a supervisor $S$ that is nonblocking and controllable with respect to the plant $G$, and we furthermore have that some of the events are unobservable.

The supervisor $\mathcal{L}(S/G)$ will remain nonblocking and controllable if it also is observable with respect to $\mathcal{L}(G)$, $\Sigma_o$ and $\Sigma_c$.

Bad news: There does not exist any algorithms that find supervisors that are nonblocking, controllable and observable.

So one resort to trial and error: Design nonblocking and controllable supervisor, test for observability, revise specs if needed, ... 

It is often useful to use observer automata for detecting observability (under Experimental algorithms in old version of Supremica).

We will not formally define observer automata, but the construction of such automata is intuitive and simple (in simple cases):

**Example 41.** Solve the latter case in the previous example using observer automata: $\Sigma = \{u, b\}$, $M = \{ub, bu\}$, $\Sigma_o = \{b\}$, and $\Sigma_c = \{b\}$, is $K_2 = \{ub\}$ observable?
Solution to Example 39

Here we start with building automata

Plant

\[
\begin{array}{c}
1 \\
\downarrow u \quad b \\
2 \\
\quad u \quad b \\
3 \\
\downarrow b \\
4
\end{array}
\]

\[
\begin{array}{c}
1 \\
\downarrow b \\
3 \\
\downarrow u \\
4 \\
2
\end{array}
\]

\[K_2\]

\[\begin{array}{c}
1 \\
\downarrow u \\
2 \\
\quad b \\
4
\end{array}\]

Observer for \(K_2\)

\[\begin{array}{c}
\{1, 2\} \\
\quad b \\
\quad \{4\}
\end{array}\]

The observer is constructed as follows: In \(K_2\) we cannot distinguish between state 1 and 2 based on the observable events, so they are together. When \(b\) has happened, we know we are at 4. In an observer for the plant we would after \(b\) not know if we are at 3 or 4, so the second state would be labeled \(\{3, 4\}\). Now we compare the states in the observer and the supervisor, and check whether there are any mismatch between in disabling and enabling controllable events. We see that at state 1 \(b\) is disabled by the controller and enabled by the observer, and we can conclude that \(K_2\) is not observable.