SOEN 342 - Sections H and II:
Software Requirements and Specifications

Iteration 2: Formal specifications

Antoine Cantin	Tuan Anh Pham	Mustafa Sameem
40211205	40213926	40190889

Saturday 4th November, 2023

1 Complete formal specification in Z

The formal specification of the system introduces the following three types:

$$\mathit{SENSOR\_TYPE}, \mathit{LOCATION\_TYPE}, \mathit{TEMPERATURE\_TYPE}$$

The system's (partial) formal specification is given in the Z language and it consists of schemas and the definitions of operations that constitute the system's exposed interface.

1.1 Schemas

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{TempMonitor}} \\ \hline
\mathit{deployed} : \mathbb{P}\ \mathit{SENSOR\_TYPE} \\
\mathit{map} : \mathit{SENSOR\_TYPE} \nrightarrow \mathit{LOCATION\_TYPE} \\
\mathit{read} : \mathit{SENSOR\_TYPE} \nrightarrow \mathit{TEMPERATURE\_TYPE} \\
\mathit{sensorRegistry} : \mathbb{P}\ \mathit{SENSOR\_TYPE} \\
\mathit{locationRegistry} : \mathbb{P}\ \mathit{LOCATION\_TYPE} \\ \hline
\mathit{deployed} \subseteq \mathit{sensorRegistry} \\
\mathit{deployed} = \operatorname{dom} \mathit{map} \\
\mathit{deployed} = \operatorname{dom} \mathit{read} \\ \hline
\end{array}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{DeploySensorOK}} \\ \hline
\Delta \mathit{TempMonitor} \\
\mathit{sensor?} : \mathit{SENSOR\_TYPE} \\
\mathit{location?} : \mathit{LOCATION\_TYPE} \\
\mathit{temperature?} : \mathit{TEMPERATURE\_TYPE} \\ \hline
\mathit{sensor?} \notin \mathit{deployed} \\
\mathit{location?} \notin \operatorname{ran} \mathit{map} \\
\mathit{deployed}' = \mathit{deployed} \cup \{\mathit{sensor?}\} \\
\mathit{map}' = \mathit{map} \cup \{\mathit{sensor?} \mapsto \mathit{location?}\} \\
\mathit{read}' = \mathit{read} \cup \{\mathit{sensor?} \mapsto \mathit{temperature?}\} \\ \hline
\end{array}$$

$$\begin{array}{l}
\textit{ReadTemperatureOK} \\
\hline
\Xi\, TempMonitor \\
location? : LOCATION\_TYPE \\
temperature! : TEMPERATURE\_TYPE \\
\hline
location? \in \operatorname{ran} map \\
temperature! = read(map^{-1}(location?)) \\
\hline
\end{array}$$

$$\begin{array}{l}
\textit{ReplaceSensorOK} \\
\hline
\Delta\, TempMonitor \\
old\ \ sensor? : SENSOR\_TYPE \\
new\ \ sensor? : SENSOR\_TYPE \\
\hline
old\ \ sensor? \in \operatorname{dom} map \\
old\ \ sensor? \in \operatorname{dom} read \\
new\ \ sensor? \in \operatorname{dom} sensorRegistry \\
new\ \ sensor? \notin deployed \\
location' = map\ (old\ \ sensor?) \\
temperature' = read\ (old\ \ sensor?) \\
deployed' = deployed \cup \{new\ \ sensor?\} \\
map' = \{old\ \ sensor?\} ⩤ map \\
read' = \{old\ \ sensor?\} ⩤ read \\
deployed' = deployed \setminus \{old\ \ sensor?\} \\
sensorRegistry' = sensorRegistry \setminus \{old\ \ sensor?\} \\
map'' = map' \cup \{new\ \ sensor? \mapsto location'\} \\
read'' = read' \cup \{new\ \ sensor? \mapsto temperature'\} \\
\hline
\end{array}$$

$$\begin{array}{l}
\textit{RemoveSensorOK} \\
\hline
\Delta\, TempMonitor \\
sensor? : SENSOR\_TYPE \\
\hline
\qquad \textit{(Case 2: Sensor is not in the deployed subset)} \\
sensor? \notin deployed \\
sensorRegistry' = sensorRegistry \setminus \{sensor?\} \\
\hline
\end{array}$$

RemoveDeployedSensorOK

$$\begin{array}{l}
\Delta TempMonitor \\
sensor? : SENSOR\_TYPE \\
\hline
\qquad \textit{(Case 1: Sensor is in the deployed subset)} \\
sensor? \in deployed \\
map' = \{sensor?\} \ndres map \\
read' = \{sensor?\} \ndres read \\
deployed' = deployed \setminus \{sensor?\} \\
sensorRegistry' = sensorRegistry \setminus \{sensor?\}
\end{array}$$

ReturnLocationTemperatureCollection

$$\begin{array}{l}
\Xi TempMonitor \\
temp : LOCATION\_TYPE \pfun TEMPERATURE\_TYPE \\
output! : \mathrm{seq}(LOCATION\_TYPE \times TEMPERATURE\_TYPE) \\
\hline
temp = \{l : LOCATION\_TYPE \mid l \in ran(map) \Rightarrow l \mapsto read(map^{-1}(l))\} \\
output! = \langle l, t : LOCATION\_TYPE \times TEMPERATURE\_TYPE \mid (l \mapsto t) \in\Rightarrow (l, t)\rangle
\end{array}$$

Success

$$\begin{array}{l}
\Xi TempMonitor \\
response! : MESSAGE \\
\hline
response! \ = \ 'ok'
\end{array}$$

SensorAlreadyDeployed

$$\begin{array}{l}
\Xi TempMonitor \\
sensor? : SENSOR\_TYPE \\
response! : MESSAGE \\
\hline
sensor? \in deployed \\
response! \ = \ 'Sensor \ deployed'
\end{array}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\_\ LocationAlreadyCovered\ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_} \\
\Xi TempMonitor \\
location? : LOCATION\_TYPE \\
response! : MESSAGE \\
\hline
location? \in \operatorname{ran} map \\
response! \ = \ 'Location\ already\ covered' \\
\hline
\end{array}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\_\ LocationUnknown\ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_} \\
\Xi TempMonitor \\
location? : LOCATION\_TYPE \\
response! : MESSAGE \\
\hline
location? \notin \operatorname{ran} map \\
response! \ = \ 'Location\ not\ covered' \\
\hline
\end{array}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\_\ SensorUnknown\ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_} \\
\Xi TempMonitor \\
sensor? : SENSOR\_TYPE \\
response! : MESSAGE \\
\hline
sensor? \notin sensorRegistry \\
response! \ = \ 'Sensor\ does\ not\ exist' \\
\hline
\end{array}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\_\ SensorNotDeployed\ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_} \\
\Xi TempMonitor \\
sensor? : SENSOR\_TYPE \\
response! : MESSAGE \\
\hline
sensor? \notin deployed \\
response! \ = \ 'Sensor\ notdeployed' \\
\hline
\end{array}$$

1.2 Operations

$$\begin{array}{l} \mathit{DeploySensor} \mathrel{\widehat{=}} \\ \quad (\mathit{DeploySensorOK} \land \mathit{Success}) \oplus \\ \quad (\mathit{SensorAlreadyDeployed} \lor \mathit{LocationAlreadyCovered}) \end{array}$$

$$\begin{array}{l} \mathit{ReadTemperature} \mathrel{\widehat{=}} \\ \quad (\mathit{ReadTemperatureOK} \land \mathit{Success}) \oplus \mathit{LocationUnknown} \end{array}$$

$$\begin{array}{l} \mathit{ReplaceSensor} \mathrel{\widehat{=}} \\ \quad (\mathit{ReplaceSensorOK} \land \mathit{Success}) \oplus (\mathit{SensorNotDeployed}) \end{array}$$

$$\begin{array}{l} \mathit{RemoveSensor} \mathrel{\widehat{=}} \\ \quad ((\mathit{RemoveDeployedSensorOK} \land \mathit{Success}) \oplus (\mathit{SensorNotDeployed})) \\ \qquad\qquad\qquad\qquad\qquad \oplus \\ \quad ((\mathit{RemoveSensorOK} \land \mathit{Success}) \oplus (\mathit{SensorUnknown})) \end{array}$$