

SOEN 342 - Sections II

Software Requirements and Specifications

Project

Vanessa DiPietrantonio 40189938

Clara Gagnon 40208598

Ahmad Elmahallawy 40193418

November 5, 2023

1 Formal specification in Z

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

$SENSOR_TYPE, LOCATION_TYPE, TEMPERATURE_TYPE$

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 and Operations given in the project

TempMonitor

$deployed : \mathbb{P} \, SENSOR_TYPE$

$map : SENSOR_TYPE \rightarrow LOCATION_TYPE$

$read : SENSOR_TYPE \rightarrow TEMPERATURE_TYPE$

$deployed = \text{dom } map$

$deployed = \text{dom } read$

DeploySensorOK

$\Delta TempMonitor$

$sensor? : SENSOR_TYPE$

$location? : LOCATION_TYPE$

$temperature? : TEMPERATURE_TYPE$

$sensor? \notin deployed$

$location? \notin \text{ran } map$

$deployed' = deployed \cup \{sensor?\}$

$map' = map \cup \{sensor? \mapsto location?\}$

$read' = read \cup \{sensor? \mapsto temperature?\}$

ReadTemperatureOK

$\exists TempMonitor$

$location? : LOCATION_TYPE$

$temperature! : TEMPERATURE_TYPE$

$location? \in \text{ran } map$

$temperature! = read(map^{-1}(location?))$

<i>Success</i>
$\exists TempMonitor$ $response! : MESSAGE$
$response! = 'ok'$

<i>SensorAlreadyDeployed</i>
$\exists TempMonitor$ $sensor? : SENSOR_TYPE$ $response! : MESSAGE$
$sensor? \in deployed$ $response! = 'Sensor\ deployed'$

<i>LocationAlreadyCovered</i>
$\exists TempMonitor$ $location? : LOCATION_TYPE$ $response! : MESSAGE$
$location? \in \text{ran } map$ $response! = 'Location\ already\ covered'$

<i>LocationUnknown</i>
$\exists TempMonitor$ $location? : LOCATION_TYPE$ $response! : MESSAGE$
$location? \notin \text{ran } map$ $response! = 'Location\ not\ covered'$

$$\begin{aligned}
DeploySensor &\hat{=} \\
& (DeploySensorOK \wedge Success) \oplus \\
& (SensorAlreadyDeployed \vee LocationAlreadyCovered)
\end{aligned}$$

$$\begin{aligned}
ReadTemperature &\hat{=} \\
& (ReadTemperatureOK \wedge Success) \oplus LocationUnknown
\end{aligned}$$

1.2 Added Schemas and Operations to Formal Specifications

$\text{MoveToNewLocationOK}$
$\Delta \text{TempMonitor}$
$\text{sensor?} : \text{SENSOR_TYPE}$
$\text{location?} : \text{LOCATION_TYPE}$
$\text{sensor?} \in \text{deployed}$
$\text{location?} \notin \text{ran map}$
$\text{map}' = \text{map} \oplus \{\text{sensor?} \mapsto \text{location?}\}$

SensorNotDeployed
$\Xi \text{TempMonitor}$
$\text{sensor?} : \text{SENSOR_TYPE}$
$\text{response!} : \text{MESSAGE}$
$\text{sensor?} \notin \text{deployed}$
$\text{response!} = \text{'Sensor not deployed'}$

$\text{LocationAlreadyOccupied}$
$\Xi \text{TempMonitor}$
$\text{location?} : \text{LOCATION_TYPE}$
$\text{response!} : \text{MESSAGE}$
$\text{location?} \in \text{ran map}$
$\text{response!} = \text{'Location already occupied'}$