

EECS3342Z-W19 Lab7 Sequential Programs

(1) In Slides 06, we specify and refine a **demanding** linear search program. The specification uses the Hoare notation:

$$\left\{ \begin{array}{l} n \in \mathbb{N} \\ 0 < n \\ f \in 1..n \rightarrow S \\ v \in \text{ran}(f) \end{array} \right\} \text{ search } \left\{ \begin{array}{l} r \in \text{dom}(f) \\ f(r) = v \end{array} \right\}$$

We also introduce the merging rules to transform a machine with a set of events into code.

(2) In slides 07, we specify and refine a tolerant linear search program.

```
{carrier set S
n ∈ ℕ
f ∈ 1..n → S
v ∈ S}
search (v)
{v ∈ ran(f) ⇒ f(r) = v
 v ∉ ran(f) ⇒ r = 0}
```

In this lab, you must (A) use Rodin to specify and refine #1 and #2. (B) Then you must use the merging rules to obtain the final code (this is done manually, not in Rodin).

Remark: The **demanding** version (#1) has a **strong** precondition, viz. that the item v we are searching for is in the array. This is easier to code.

The **tolerant** version has a weak precondition viz. that the item v may not be in the array. This version requires more **defensive** code.

The tolerant version and the merging rules are also in the textbook available in the SVN. Note that we are using relational image in the specification. You may wish to review notation in slides 05.