WAREHOUSE SHARED RESOURCE

CADT WarehouseAccessControl
OPERATIONS
ACTION enterWarehouse: $\mathbb{N}[i] \times \mathbb{N}[i]$
ACTION exitWarehouse: $\mathbb{N}[i] \times \mathbb{N}[i]$

SEMANTICS
DOMAIN:
STATE: $(weight : Warehouse \to Weight \times occupied : Warehouse \to \mathbb{B})$
TYPE: $Warehouse = 0 \ldots \text{N\_WAREHOUSES} - 1$
$Weight = 0 \ldots \text{MAX\_WEIGHT\_IN\_WAREHOUSE}$
INITIAL: $\forall n \in Warehouse \bullet weight(n) = 0 \land \neg occupied(n)$
INVARIANT: $\forall n \in Warehouse \bullet weight(n) \leq \text{MAX\_WEIGHT\_IN\_WAREHOUSE}$

PRE: $n \in \{0 \ldots \text{N\_WAREHOUSES} - 1\} \land w \in \{0 \ldots \text{MAX\_WEIGHT\_IN\_WAREHOUSE} - 1\}$
CPRE: $w + weight(n) \leq \text{MAX\_WEIGHT\_IN\_WAREHOUSE}$
enterWarehouse(n,w)
POST: $weight = weight^{\text{in}} \oplus \{n \mapsto weight^{\text{in}}(n) + w\} \land$
$(n > 0 \Rightarrow occupied = occupied^{\text{in}} \oplus \{n \mapsto \text{False}\}) \land$
$(n = 0 \Rightarrow occupied = occupied^{\text{in}})$

PRE: $n \in \{0 \ldots \text{N\_WAREHOUSES} - 1\} \land w \in \{0 \ldots \text{MAX\_WEIGHT\_IN\_WAREHOUSE} - 1\}$
CPRE: $n = \text{N\_WAREHOUSES} - 1 \lor \neg occupied(n + 1)$
exitWarehouse(n,w)
POST: $weight = weight^{\text{in}} \oplus \{n \mapsto weight^{\text{in}}(n) - w\} \land$
$(n < \text{N\_WAREHOUSES} - 1 \Rightarrow occupied = occupied^{\text{in}} \oplus \{n + 1 \mapsto \text{True}\}) \land$
$(n = \text{N\_WAREHOUSES} - 1 \Rightarrow occupied = occupied^{\text{in}})$