Métodos Formales

Especificación Formal y Validación de un Sistema de Detección de Metales Pesados en el Agua

Por María Fernanda Pinazo, Aldo Vasquez, Josué Ramos, Fernando Pérez, Juan Quispe

Model Checking

- Para nuestro sistema de detección de metales pesados, se define un modelo que involucra dos subsistemas independientes que aseguran no estar simultáneamente en estado de alerta.

Variables del Modelo

- System1: Puede estar en los estados AlertaOn o AlertaOff.
- System2: Puede estar en los estados AlertaOn o AlertaOff.

Transiciones del Modelo

System1

- Desde AlertaOff, puede ir a AlertaOn o permanecer en AlertaOff.
- Desde AlertaOn, solo puede ir a AlertaOff.

System2

- Desde AlertaOff, puede ir a AlertaOn o permanecer en AlertaOff.
- Desde AlertaOn, solo puede ir a AlertaOff.

Volver

Especificaciones del Modelo

Volver

CTL

- AG¬(System1 = AlertaOn ∧ System2 = AlertaOn): Siempre es cierto que ambos sistemas no están en estado AlertaOn simultáneamente.
- EF System1 = AlertaOn: Eventualmente, el sistema 1 llega al estado AlertaOn.
- EF System2 = AlertaOn: Eventualmente, el sistema 2 llega al estado AlertaOn.
- AG (System1 = AlertaOff → AX System1 = AlertaOn): Si System1 esta en AlertaOff, en el siguiente estado puede ir a AlertaOn.

LTL

- F (System1 = AlertaOn): En algun momento, System1 estara en AlertaOn.
- G (System1 = AlertaOn → X System1 = AlertaOff): Siempre que System1 este en AlertaOn, cambiara a AlertaOff en el siguiente estado.

Descripción del Modelo

Volver

```
MODULE main
VAR
  System1 : {AlertaOn, AlertaOff}; -- Sistema 1 puede estar en AlertaOn o AlertaOff
  System2 : {AlertaOn, AlertaOff}; -- Sistema 2 puede estar en AlertaOn o AlertaOff

ASSIGN
  -- Inicialización de los sistemas
  init(System1) := AlertaOff;
  init(System2) := AlertaOff;

  -- Transiciones para System1
  next(System1) := case
    System1 = AlertaOff : {AlertaOn, AlertaOff}; -- Desde AlertaOff puede ir a AlertaOn o quedarse en AlertaOff
    System1 = AlertaOn : {AlertaOff};            -- Desde AlertaOn solo puede ir a AlertaOff
    TRUE : System1;                              -- Default (por seguridad)
  esac;

  -- Transiciones para System2
  next(System2) := case
    System2 = AlertaOff : {AlertaOn, AlertaOff}; -- Desde AlertaOff puede ir a AlertaOn o quedarse en AlertaOff
    System2 = AlertaOn : {AlertaOff};            -- Desde AlertaOn solo puede ir a AlertaOff
    TRUE : System2;                              -- Default (por seguridad)
  esac;
```

Descripción del Modelo

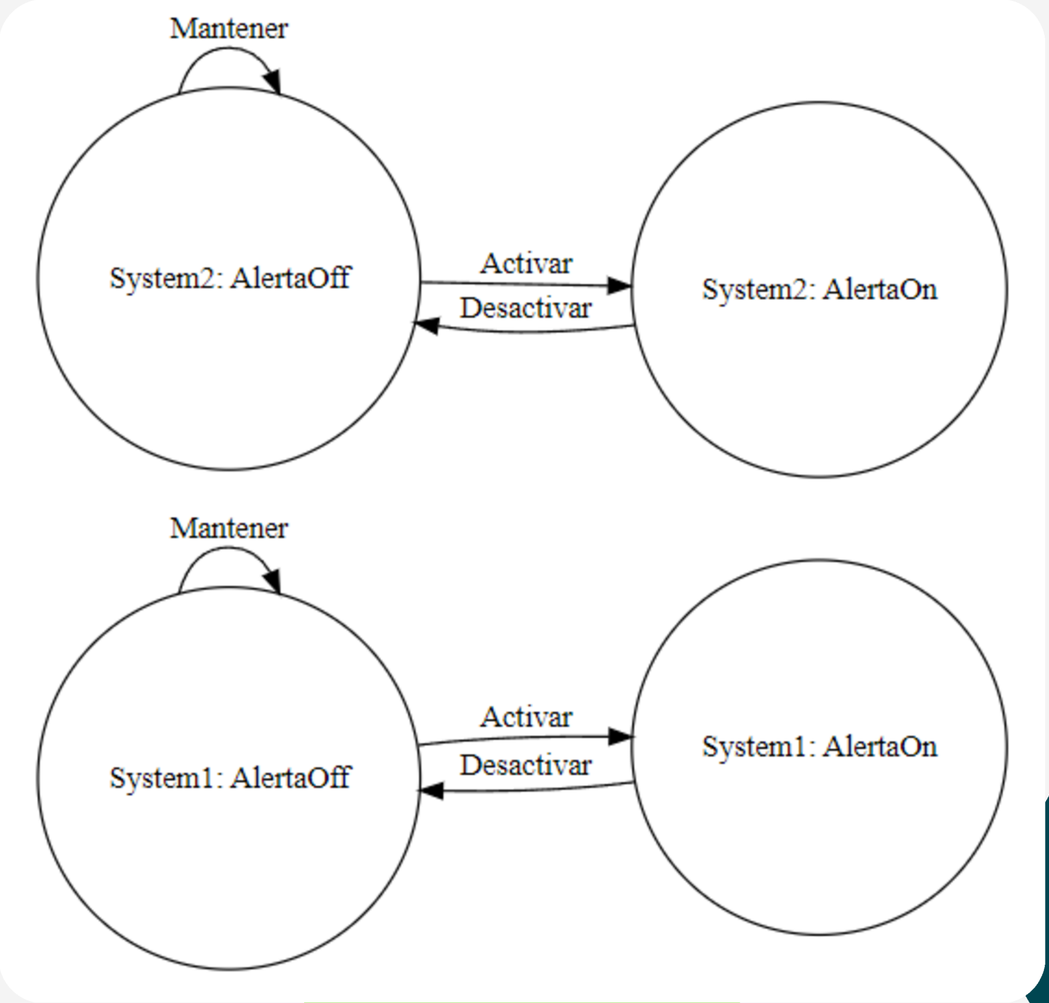
Volver

```
  -- Transiciones para System2
  next(System2) := case
    -- Desde AlertaOff puede ir a AlertaOn o quedarse en AlertaOff
    System2 = AlertaOff : {AlertaOn, AlertaOff};
    -- Desde AlertaOn solo puede ir a AlertaOff
    System2 = AlertaOn : {AlertaOff};
    -- Default (por seguridad)
    TRUE : System2;
  esac;

-- Especificaciones en CTL
-- Siempre es cierto que ambos sistemas no están en "AlertaOn" al mismo tiempo.
SPEC AG !(System1 = AlertaOn & System2 = AlertaOn)
-- Eventualmente, el sistema 1 llega al estado "AlertaOn".
SPEC EF System1 = AlertaOn
-- Eventualmente, el sistema 2 llega al estado "AlertaOn".
SPEC EF System2 = AlertaOn
-- Si System1 está en "AlertaOff", en el siguiente estado puede ir a "AlertaOn".
SPEC AG (System1 = AlertaOff -> AX System1 = AlertaOn)

-- Especificaciones en LTL
-- En algún momento, System1 estará en "AlertaOn".
LTLSPEC F (System1 = AlertaOn)
-- Siempre que System1 esté en "AlertaOn", cambiará a "AlertaOff" en el siguiente estado.
LTLSPEC G (System1 = AlertaOn -> X System1 = AlertaOff)
```

Diagrama de transición de Estados



¡MUCHAS GRACIAS!