Análisis Automático basado en SAT aplicado a la Validación de Requisitos de Software

Renzo Degiovanni

Departamento de Computación, FCEFQyN, Universidad Nacional de Río Cuarto
Río Cuarto, Córdoba, Argentina
rdegiovanni@dc.exa.unrc.edu.ar

Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina

06 de Diciembre de 2010

Qué hacemos?

Área de Trabajo

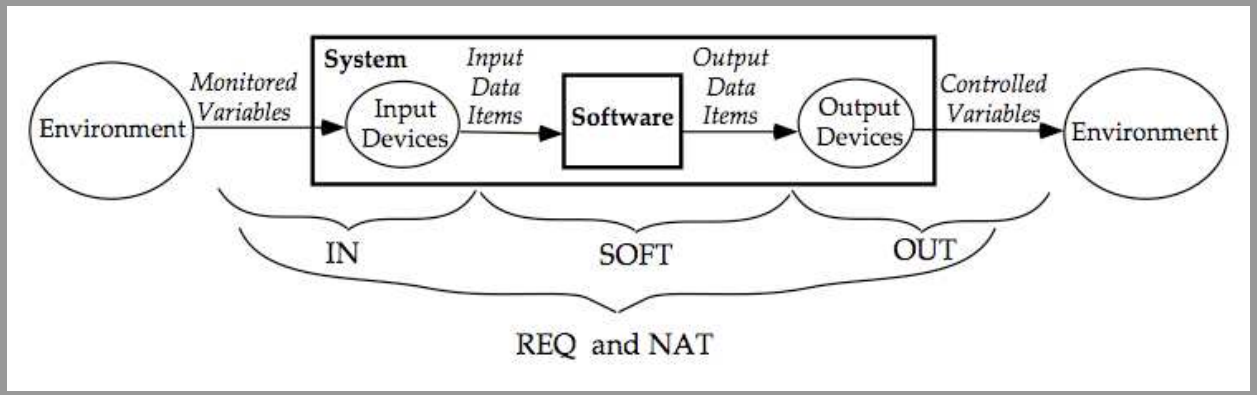
Trabajamos en el área de métodos formales, en particular, en una subárea conocida como *métodos formales livianos*. Éstos apuntan a la simplicidad de aplicación y a la automatización del proceso de verificación.

Validación de requisitos de software

- Existe una amplia variedad de notaciones para la descripción de requisitos de software, pero aquellas con una semántica formal son particularmente apropiadas para el análisis.
- En particular, la notación tabular de Parnas y el método Software Cost Reduction (SCR) resultan convenientes para la descripción formal de requisitos.

Software Cost Reduction (SCR)

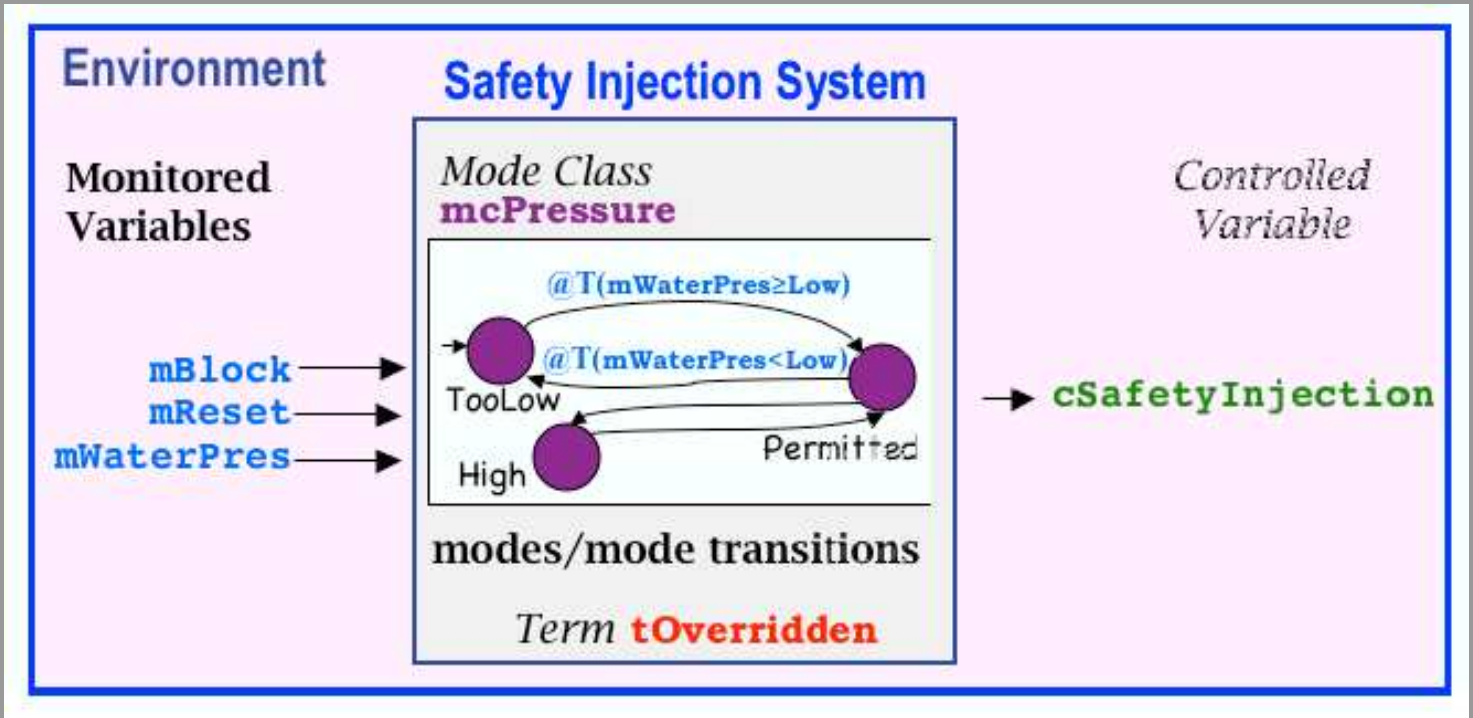
El modelo para la especificación de requisitos en SCR puede describirse de la siguiente manera:



Las tablas son utilizadas para describir formalmente las relaciones **REQ** y **NAT**.
REQ relación entre vars. monitoreadas y controladas que el sistema debe implicar.
NAT relación entre vars. monitoreadas y controladas que se dan debido a restricciones naturales.

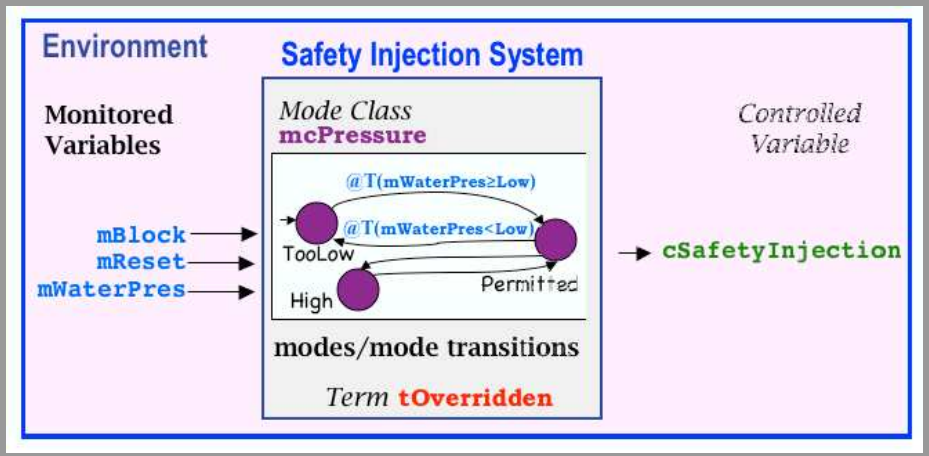
Un Simple Ejemplo

Safety Injection System (SIS) es un sistema de control para refrigerar un núcleo de una planta nuclear.



Un Simple Ejemplo

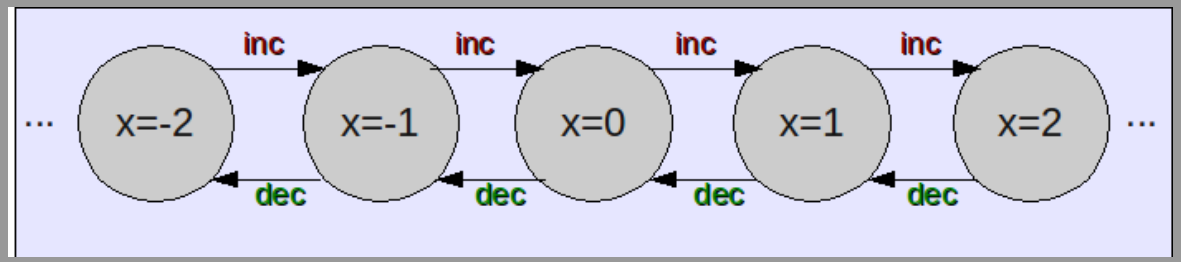
Safety Injection System (SIS) es un sistema de control para refrigerar un núcleo de una planta nuclear.



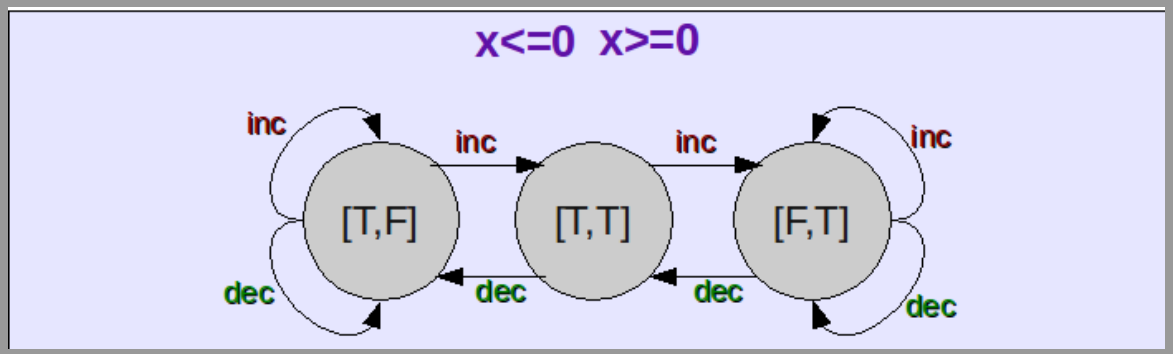
Old Mode	Event	New Mode
TooLow	@T(WaterPres $\geq$ Low)	Permitted
Permitted	@T(WaterPres $\geq$ Permit)	High
Permitted	@T(WaterPres $<$ Low)	TooLow
High	@T(WaterPres $<$ Permit)	Permitted

Abstracción

Modelo concreto

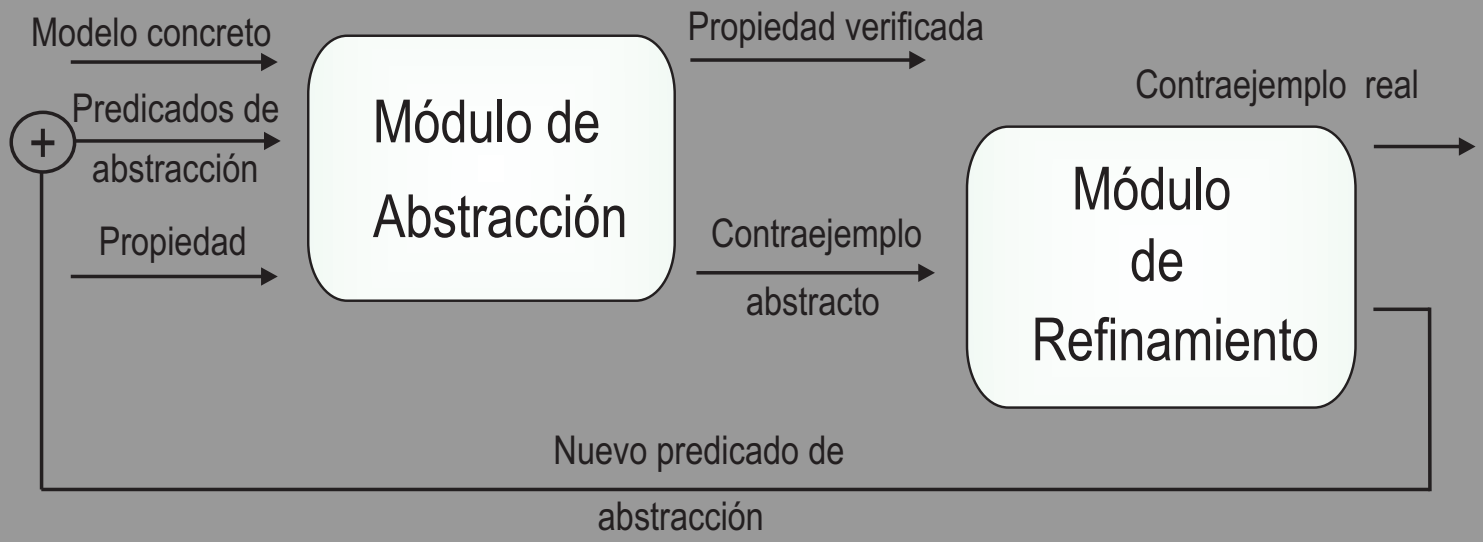


Modelo abstracto

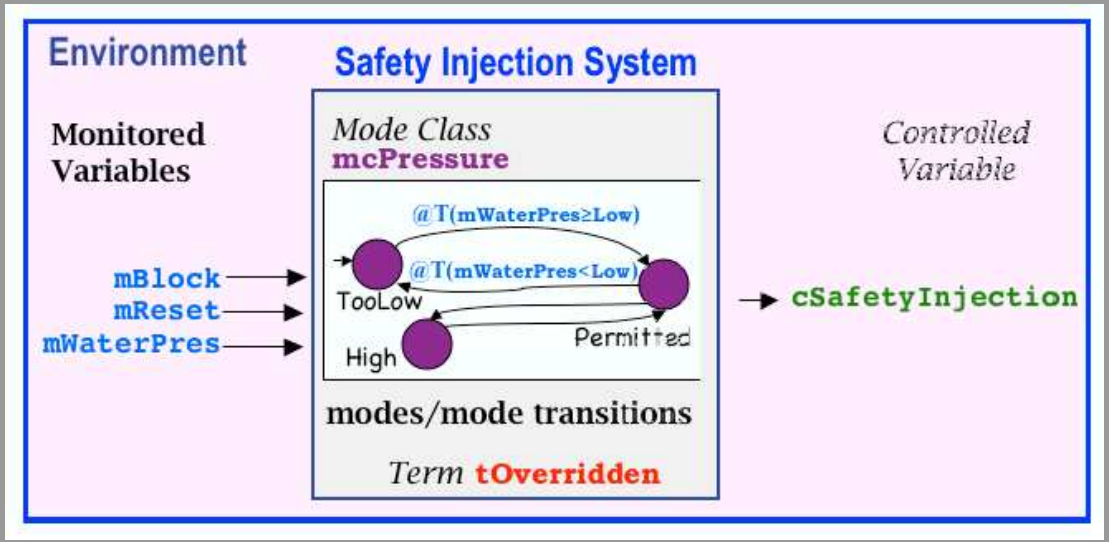


Abstracción por predicados

Abstracción por Predicados “in a nutshell”



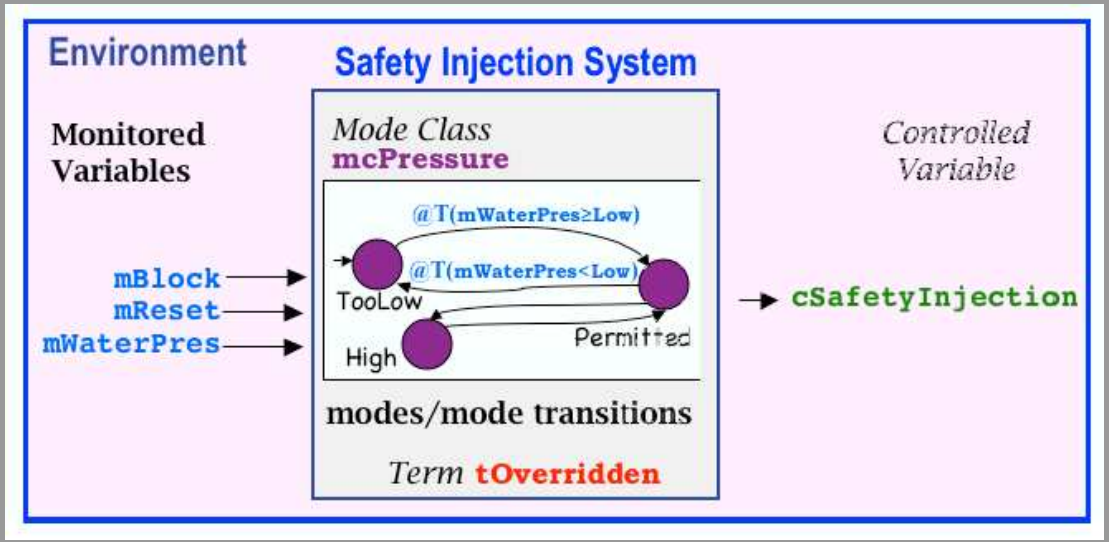
Nuestros propósitos...



- Realizar análisis aprovechando la estructura tabular de las especificaciones.

+ **Los modos dan una abstracción inicial.**

Nuestros propósitos...



- Realizar análisis aprovechando la estructura tabular de las especificaciones.

\+ **Los modos dan una abstracción inicial.**