ASRC: Charla sobre seguridad:

Título: Safety critical computer systems.
Profesor: Dr. Matthias F. Wagner.

SCS (Safety Critical Systems) ponen en peligro:
- la vida humana
- la salud
- el medio ambiente.

También pueden poner en peligro la existencia de una organización que dependa de ellos. Ambos son controlados por software. (Ejemplo de una máquina de resonancia magnética nuclear.)

Riesgo y sociedad:
Estar totalmente seguros es imposible, por lo que hay que establecer ciertos objetivos en función de una prioridad.

Algo seguro es algo que no pone en riesgo la vida humana.
Un sistema relacionado con la seguridad es aquel que asegura.
SCS tiene influencia directa con la seguridad.
Un fallo en un defecto en un sistema.
La presencia de un defecto (hardware o software) puede llevar a un error. Este es el mecanismo por el cual los defectos son aparentes.
Los defectos más randoms son asociados a fallos en los componentes hardware.
Los defectos sistemáticos incluyen especificación y diseño de defectos. Este es el verdadero defecto software.
La confiabilidad es la probabilidad de un sistema de funcionar bien teniendo en cuenta ciertas condiciones.
La disponibilidad es la probabilidad de un sistema de funcionar bien en un cierto tiempo.
Un peligro es una situación en la cual existe un riesgo potencial.
Un riesgo es una combinación de probabilidades de un evento peligroso y que conlleva severas consecuencias.
Un accidente causa severos daños.
La seguridad está libre de accidentes o perdidas.
La seguridad está libre de acciones maliciosas.

La centralización es un factor de riesgo.
Muchos fallos son debidos al incremento de la complejidad que es, a su vez, un obstáculo para la seguridad.

Un sistema que sea intelectualmente inmanejable debido al nivel de interacciones que requiere es difícil de planear, entender, anticiparse, etc.
Por lo tanto, el objetivo principal es controlar al complejidad imponiendo límites intelectuales.

Un sistema seguro no es lo mismo que un sistema confiable.
Un sistema confiable requiere diferentes desarrollos que un ingeniero tiene como objetivo.

La falta de restricciones apropiadas en el diseño de un computador es una de los principales problemas de seguridad.
Los errores más relacionados con software es debido a los requisitos y no al código de los programas.

Análisis de peligros:

La definición de un sistema organizado en cuanto a la complejidad es aquel que establece componentes que luego actuaran como un todo.
El análisis de peligros investiga factores relacionados con accidentes.
En el desarrollo se identifican peligros potenciales y condiciones de las que se pueden aprender para eliminarlos o controlarlos.

Dentro de los métodos de análisis de problemas nos centraremos en “Fault Tree Analysis (FTA)”.
Se centra en analizar las causas de los problemas, no de identificarlos, por lo tanto podemos mejorar el software que causa dichos problemas.
Las limitaciones de los sistemas muchas veces son producidas por errores humanos. La mayoría de los accidentes engloba la migración sistemática u organizacional de la empresa que tiene dicho software.

Los pasos de STAMP son:
- Identificar los problemas.
- Crear controles de segudirdad.
- Observar las interacciones del sistema.

Un plan de sistema seguro basado en identificar los contratos de seguridad del sistema consiste en diseñar un software con criterios y requisitos pruebas y HMI.