Sistemas críticos (SC)

Máster Universitario en Tecnología de Informática

ETSIIT, Universidad de Granada

Curso 2019-2020

Temario teor
ía

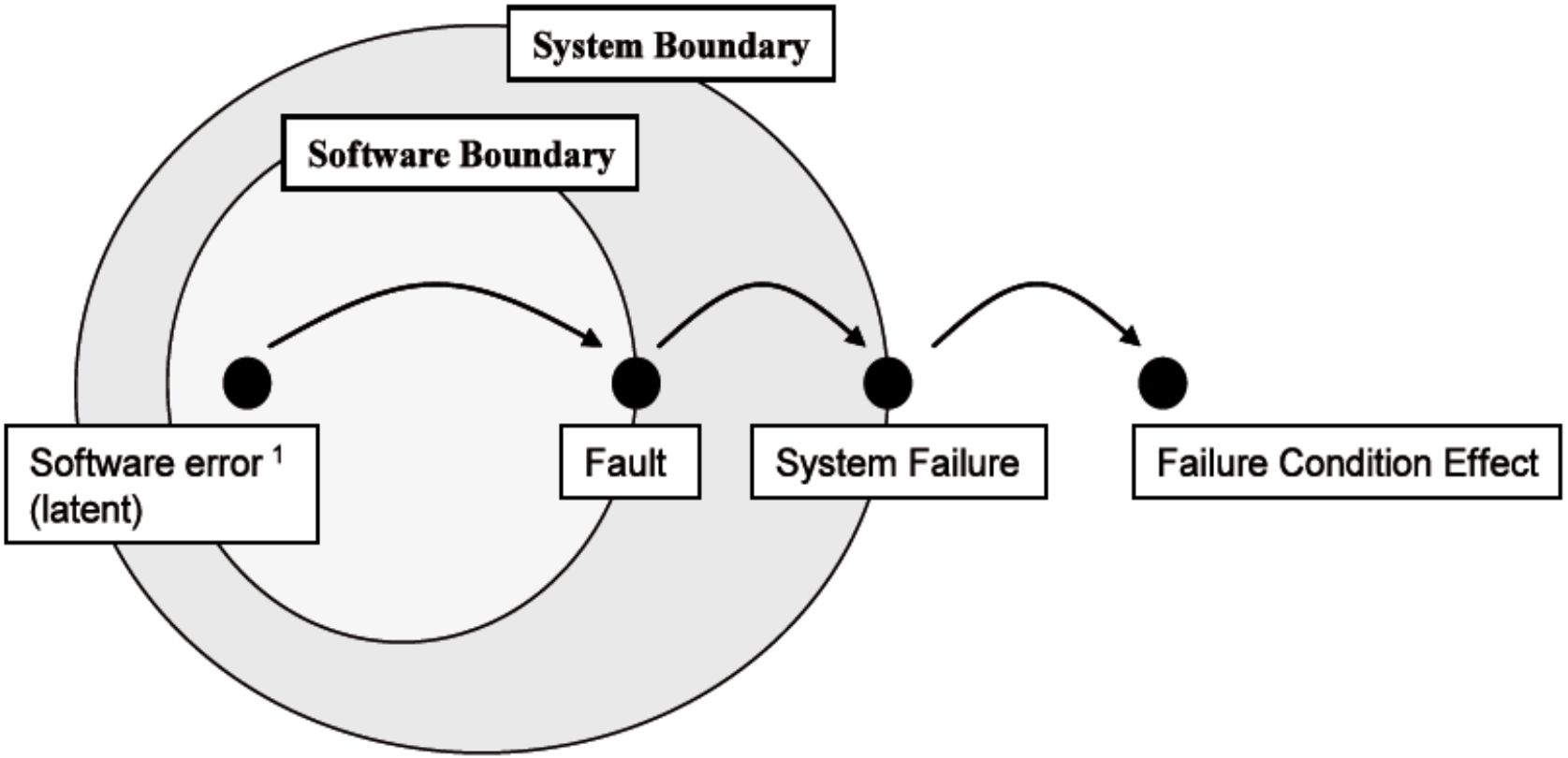
1. Introducci
2. ón y conceptos generales.
3. Metodolog
4. ías de desarrollo: flujos de diseño, requisitos y especificaciones, validación vs. Verificación, etc.
5. Dise
6. ño de plataformas para sistemas empotrados. Revisión de conceptos generales. Soluciones comerciales y open source. Codiseño hardware/software. Redundancía/fiabilidad vs. coste. Diversidad, compartición de recursos. Diseño tolerante a fallos.
7. Programaci
8. ón y desarrollo de aplicaciones. Revisión de conceptos generales. Soluciones comerciales y open source. Características para sistemas críticos

Sistemas críticos

Dependability (confiable) = Safety + realiability + availability + secure

- Fiabilidad (reliability)
- – mantenimiento del correcto servicio en el tiempo
- Disponibilidad (availability)
- – prontitud en el uso
- Sin riesgos (safety)
- – fallos controlados y sin consecuencias catastróficas
- Seguridad (security)

Sistemas críticos



Sistemas críticos

- Safety critical systems
- Mixed-criticality

} Certificación (ej. Aviónica)

DAL	Definition : Software whose anomalous behavior [...] would cause or contribute to a failure [...] resulting in a
A	**catastrophic** failure condition for the aircraft
B	**hazardous/severe-major** failure condition for the aircraft
C	**major** failure condition for the aircraft
D	**minor** failure condition for the aircraft
E	**no** effect on aircraft operational capability or pilot workload

Sistemas cr íticos

TABLE 1 - Failure Condition Severity as Related to Probability Objectives and Assurance Levels

Probability (Quantitative)		Per flight hour 1.0	1.0E-3	1.0E-5	1.0E-7	1.0E-9
Probability (Descriptive)	FAA	Probable		Improbable		Extremely Improbable
	JAA	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Failure Condition Severity Classification	FAA	Minor		Major	Severe Major	Catastrophic
	JAA	Minor		Major	Hazardous	Catastrophic
Failure Condition Effect	FAA & JAA	- slight reduction in safety margins - slight increase in crew workload - some inconvenience to occupants		- significant reduction in safety margins or functional capabilities - significant increase in crew workload or in conditions impairing crew efficiency - some discomfort to occupants	- large reduction in safety margins or functional capabilities - higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely - adverse effects upon occupants	- all failure conditions which prevent continued safe flight and landing
Development Assurance Level	ARP 4754	Level D		Level C	Level B	Level A

Note: A "No Safety Effect" Development Assurance Level E exists which may span any probability range.

Failure Condition Severity (Fuente[ARP4761])

Problema de la definición

SystemC modeling and HW/SW codesign

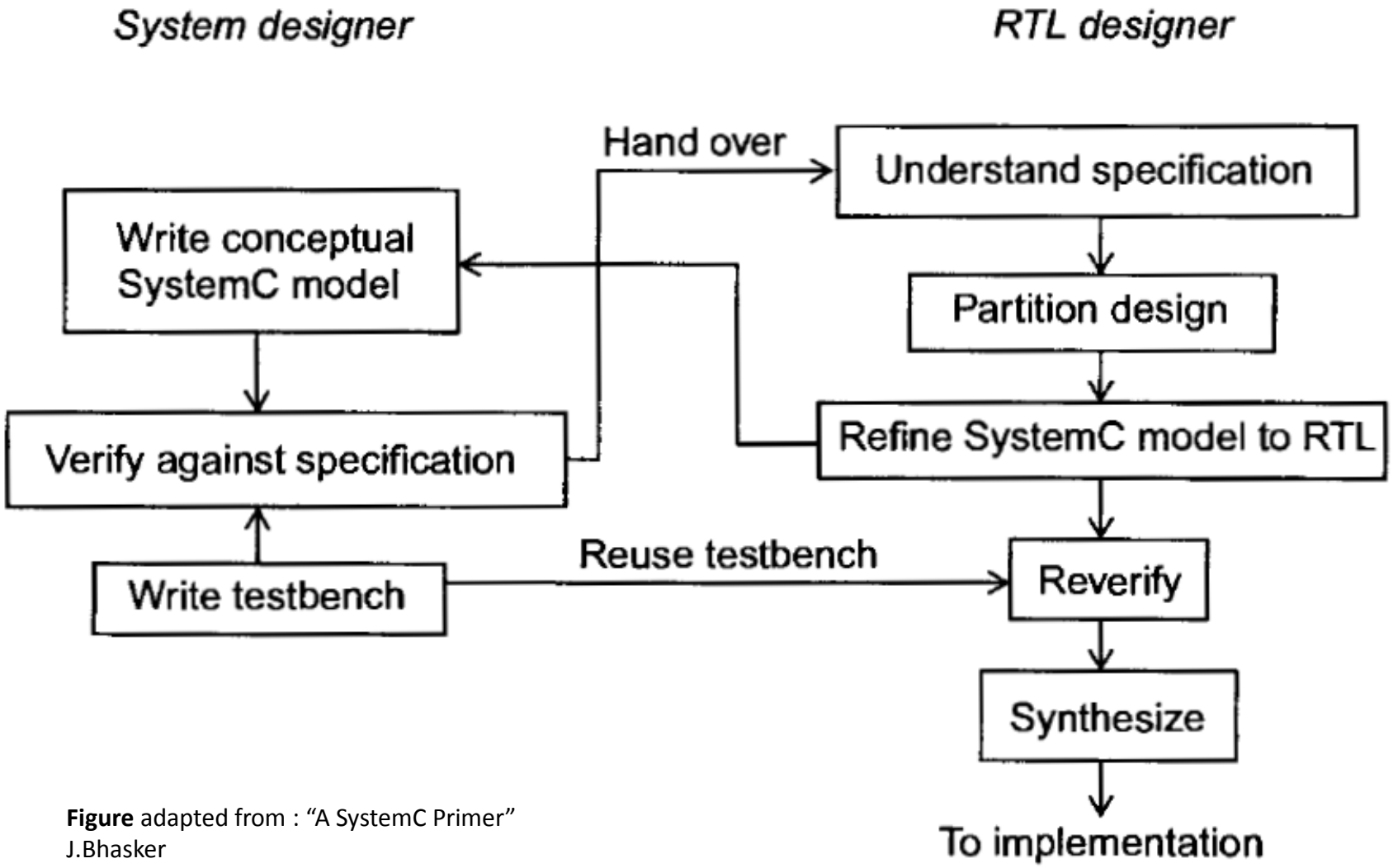


Figure adapted from : "A SystemC Primer" J.Bhasker

CASO PRÁCTICO

PROYECTO RECOMP

recomp

Preguntas

¿?