DMA e Introducción a la IEC61508

Agenda.

- DMA
- DMA en LPC1769
- IEC 61508.
  - Equipo bajo control
  - Riesgo.
  - Ciclo de vida.
  - Análisis de riesgo
  - Riesgo tolerable.
  - Niveles de Integridad de seguridad

Manejo de E/S por DMA

- Los sistemas de acceso directo a memoria (DMA) son sistemas que pueden controlar la memoria del sistema sin el uso de la CPU.
- Dado un evento determinado el módulo de DMA puede mover datos entre diferentes zonas de memoria.
- Si bien es menos flexible que la CPU, es mucho más rápido en la copia de datos que la CPU

E/S por DMA

- Algunos periféricos pueden generar grandes cantidades de datos (ADC, DAC, Ethernet, etc.).

- Las transferencias por DMA son las más adecuadas para grandes volúmenes de datos o bien para altas tasas de datos.

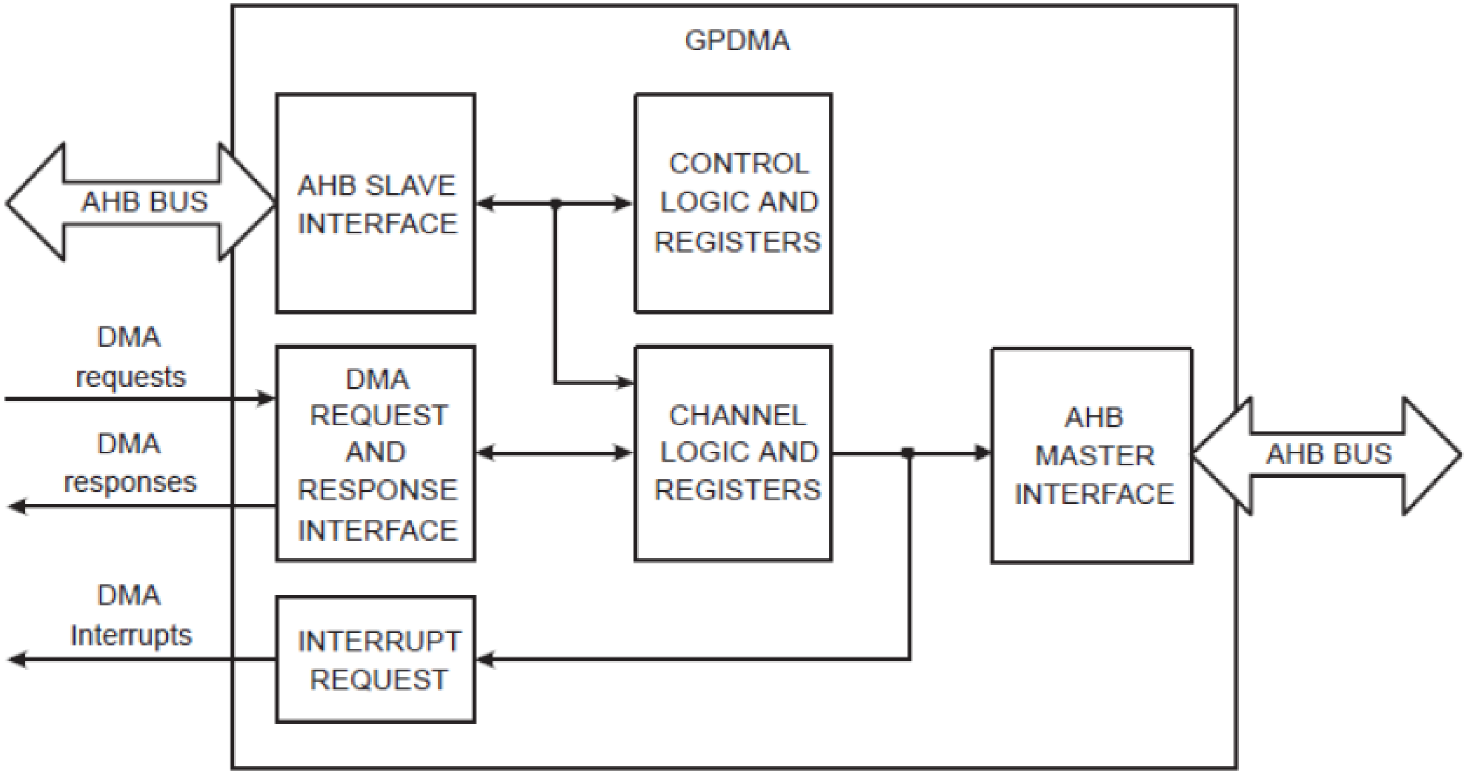
DMA. Generalidades.

- Los sistemas de DMA pueden funcionar de diferentes formas:
  - ***Transferencia única.*** Un byte, word, doble-word se transfiere por operación de DMA. Se suele utilizar en dispositivos de flujo de caracteres. Cada transferencia deshabilita la CPU.
  - ***Transferencias por bloques***. El módulo transfiere un bloque completo de memoria, mientras que la CPU no se encuentra activa.
  - ***Transferencia por ráfaga.*** El módulo de DMA transfiere un bloque de memoria, pero no desactiva la CPU, sino que alterna los accesos a la memoria con ésta

DMA en LPC176x

- El controlador de DMA se denomina GDMA.
- Soporta transferencias memoria a memoria, memoria a periférico, periférico a memoria y periférico a periférico.
- Tiene 8 canales de DMA. Cada canal soporta transferencias en una única dirección.
- Soporta scatter-gather DMA. Esto es, que puede transferir bloques de memoria no contiguos (útil para listas enlazadas).
- Soporta transferencias de 8, 16 y 32 bits

DMA en LPC176x



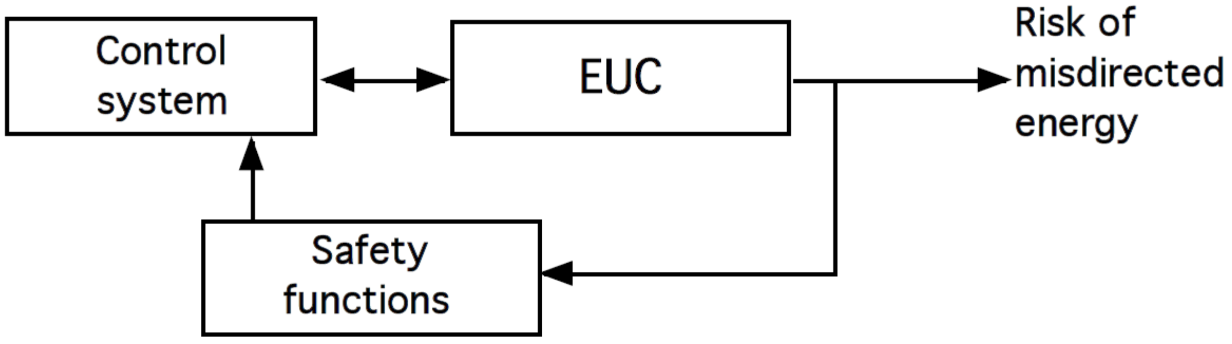
Manos a la obra

- Tome el código “ejemploDMA_Memoria.zip” este código copia un bloque de memoria a otro bloque de memoria de 16Kbytes ambos. Tiene dos modos de funcionamiento, con DMA y sin DMA. Ejecútelo en ambos modos y determine:
  - Estimaciones de BCET y WCET para ambos modos.
  - ¿Encuentra diferencias? Determine la carga de la CPU para ambos modos y determine la planificabilidad de ambos.

Manos a la obra (2)

- Tome el código “ejemploDMA_DAC.zip” Este código genera una señal analógica en el pin 0.26 del LPC1769. También tiene dos modos de funcionamiento, por DMA y por CPU. Ejecútelo en ambos modos y determine:
  - Estimaciones de BCET y WCET para ambos modos.
  - Cuál es el período de la señal generada para cada modo.
  - ¿Es posible generar la señal con el período de modo DMA en modo CPU? ¿Qué debería cambiar? ¿Con que carga de CPU?

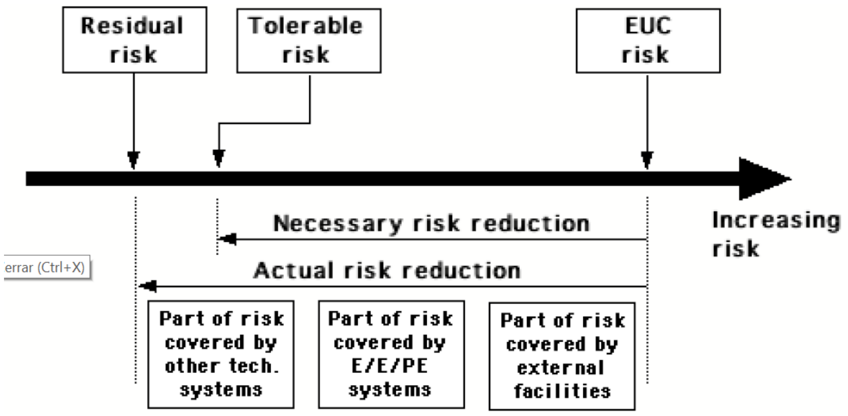
IEC61508



- La norma IEC 61508 se publica en 1998.
- La principal característica de de la norma es que introduce el concepto de que el equipo bajo control (equipment under control) implementa una ***función.***
- El estándar hace énfasis en ***la reducción de riesgos en las funciones de seguridad.***
- Las funciones de seguridad son implementadas en ***sistemas de protección***

Riesgo

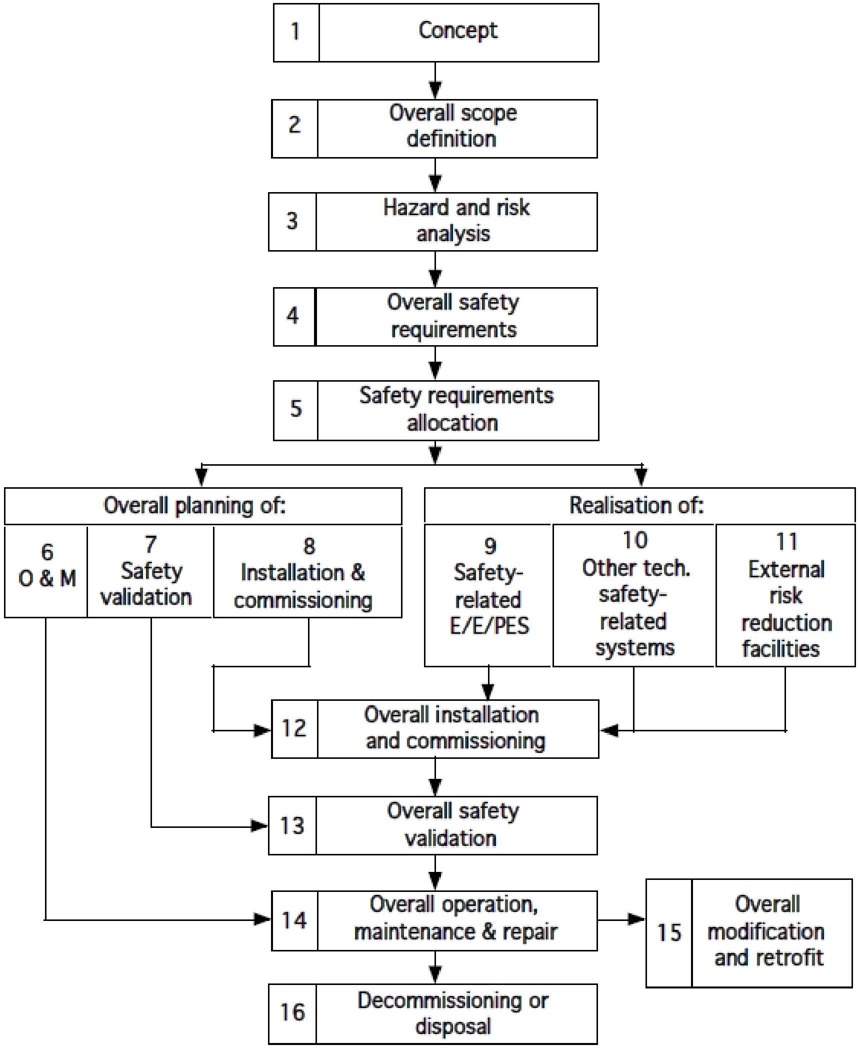
- La norma utiliza el concepto de riesgo y la definición de:
  - Riesgo actual.
  - Riesgo tolerable (El que se considera adecuado para la aplicación)
  - Riesgo residual ya que conceptualmente ***nunca se alcanza riesgo cero.***
- La reducción de riesgo se puede dar por la utilización de mecanismos distintos o ***diversos.***



Ciclo de vida

- La norma define un conjunto de ***buenas prácticas*** y recomendaciones pero no asume la responsabilidad de la seguridad por el diseño.
- La IEC61508 no es una norma para el desarrollo, pero si es una norma para la gestión de la seguridad a lo largo de la ***vida de un proyecto.***
- La norma define el ciclo de vida como un conjunto de etapas que deben cumplirse para pasar a la etapa siguiente en el desarrollo del proyecto.

Ciclo de vida



Análisis de riesgo

- Una parte importante de la norma, son los requerimientos de seguridad que se obtienen a partir del análisis de riesgo que posee el equipo bajo control y su sistema de control.
- El análisis de riesgo define tres etapas:
  - Identificación de peligros (hazard)
  - Análisis de peligros probables.
  - Asignación de riesgos
- Se define como peligro a una ***potencial fuente de daño.***
- Un equipo bajo control posee muchos potenciales peligros con su correspondiente riesgo

Análisis de riesgo (2)

Table 1: Defining categories of likelihood of occurrence

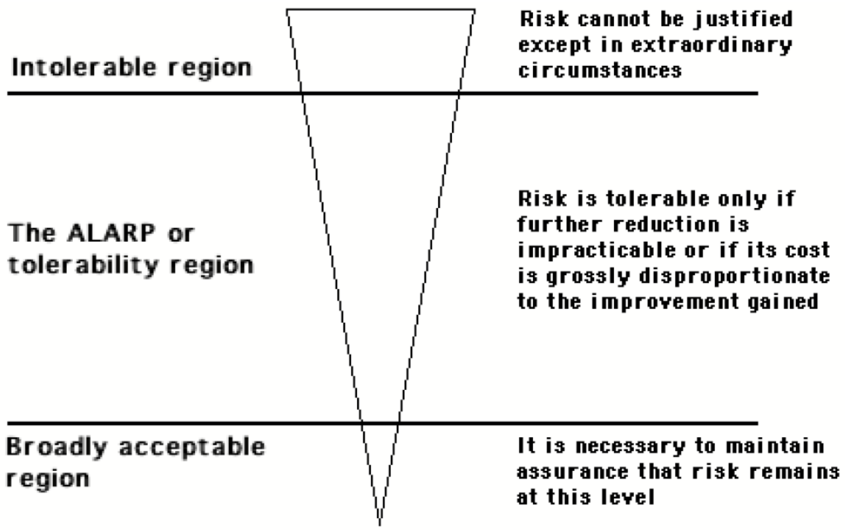
Category	Definition	Range (failures per year)
Frequent	Many times in system lifetime	$> 10^{-3}$
Probable	Several times in system lifetime	10^{-3} to 10^{-4}
Occasional	Once in system lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in system lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	$< 10^{-7}$

Table 2: Defining consequence categories

Category	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst

Riesgo tolerable.

- Para cuestiones de software el análisis de riesgo suele ser cualitativo ya que el software suele fallar de manera sistemática.
- Por lo que la pregunta es ¿Cuál es el riesgo tolerable?
- Lo que es tolerable para una aplicación puedo no serlo para otra.
- Se define lo que se conoce como principio ALARP (as low as reasonably practicable – tan bajo como sea razonablemente posible).



Clases de riesgo.

LIKELIHOOD	CONSEQUENCE Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

- Una forma de aplicar el análisis de riesgo es a través de las ***clases de riesgo.***
  - Clase 1. Inaceptable bajo cualquier circunstancia.
  - Clase 2. Indeseable, solamente tolerable si la reducción de riesgo es impracticable o excesivamente costosa
  - Clase 3. Tolerable si el costo de reducción del riesgo excede a la mejora.
  - Clase 4. Tolerable, pero debe ser monitoreado.
- Estas consideraciones nos generan la matriz de riesgo de la derecha.

Niveles de integridad de seguridad

- La norma define a la integridad de seguridad como ***la probabilidad de un sistema relacionado con la seguridad de realizar su función satisfactoriamente en cualquier condición en un período de tiempo dado.***
- Los niveles de integridad de seguridad (SIL) no son una medida de riesgo, sino una medida de la confiabilidad del sistema.
- Se definen cuatro niveles de integridad de seguridad.

Niveles de integridad de seguridad

Table 5: Safety integrity levels

Safety Integrity Level	Low Demand Mode of Operation (Pr. of failure to perform its safety functions on demand)	Continuous/High-demand Mode of Operation (Pr. of dangerous failure per hour)
4	>= 10^{-5} to 10^{-4}	>= 10^{-9} to 10^{-8}
3	>= 10^{-4} to 10^{-3}	>= 10^{-8} to 10^{-7}
2	>= 10^{-3} to 10^{-2}	>= 10^{-7} to 10^{-6}
1	>= 10^{-2} to 10^{-1}	>= 10^{-6} to 10^{-5}

IEC61508. Resumen

- La norma trata la gestión de la seguridad de un sistema programable a lo largo de toda su vida, desde su diseño hasta su desmantelamiento.
- Al igual que la mayoría de las normas no pone condiciones en el desarrollo en sí, sino principalmente en la gestión del sistema.
- Es clave para la norma el concepto de riesgo, pero también la definición de requerimientos en función de la aplicación.

Bibliografía.

- Sistemas Operativos. Diseño e Implementación. Andrew S. Tanenbaum.
- Sistemas de Tiempo Real y Lenguajes de Programación. Alan Burns, Andy Wellings. Tercera Edición. Addison Wesley.
- [IEC 1998] Draft Standard IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. International Electrotechnical Commission, Geneva, 1998