Introduzione alle normative generali sulla Safety per le Macchine

Soluzioni applicative ed esempi

Massimiliano Ruggeri

Safety in ambito automotive: un processo maturo

Si basa su strategie che lavorano in parallelo a diversi livelli sul sistema:

LIVELLO 3
Safety di livello supervisione: basata su strategie di controllo delle funzionalità dei sistemi elettronici programmabili e dei loro componenti interni, si basa sulla ridondanza hardware elettronica e prevede sempre la presenza di almeno due sistemi elettronici programmabili in comunicazione tra loro nella stessa unità di controllo.

LIVELLO 2
Safety di livello funzionale: basata su strategie software e funzionali, si basa sulla ridondanza funzionale per il calcolo delle attuazioni che il sistema deve erogare in real time, si basa sulla diversity

LIVELLO 1
Safety di livello hardware: basata su componenti, si basa sulla ridondanza fisica di Componenti safety critical, siano essi sensori, attuatori o dispositivi non elettronici

Sfruttare la Diversity nella Redundancy

La norma IEC 61508 ci consiglia di sfruttare la Diversity, lo stesso concetto è ora enunciato e fortemente consigliato in caso di presenza di sistemi elettronici programmabili nella ISO 13849. La Diversity è una delle chiavi più importanti della robustezza del sistema elettronico e va gestita a tutti i livelli con tecniche il più possibile differenziate:

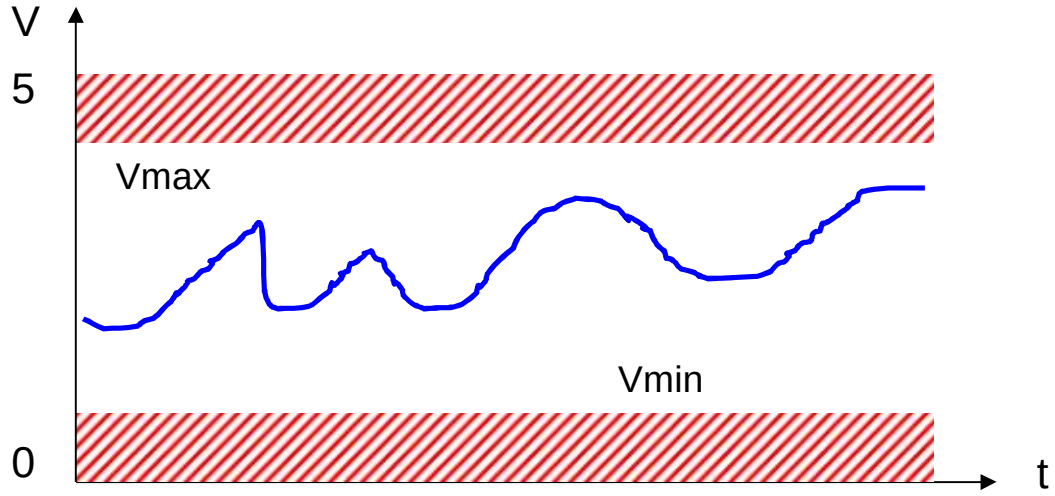
1. Diversity nelle acquisizione sia di informazioni da sensori che informazioni di stato (tipicamente input digitali)
2. Diversity nella esecuzione delle strategie di controllo e nella loro verifica
3. Diversity nella gestione delle attuazioni e della loro abilitazione

Riconoscimento dei Guasti

Il riconoscimento del singolo guasto è appannaggio di strategie di controllo molto diversificate che devono necessariamente rapportarsi alla fisica del fenomeno sotto osservazione e ai metodi di osservazione dello stesso.

Si può sempre avere la possibilità di monitorare lo stato di un **sensore** se si ha cura di sceglierlo tale che in funzionamento normale non possa utilizzare tutto il campo di valori acquisibile dal micro:

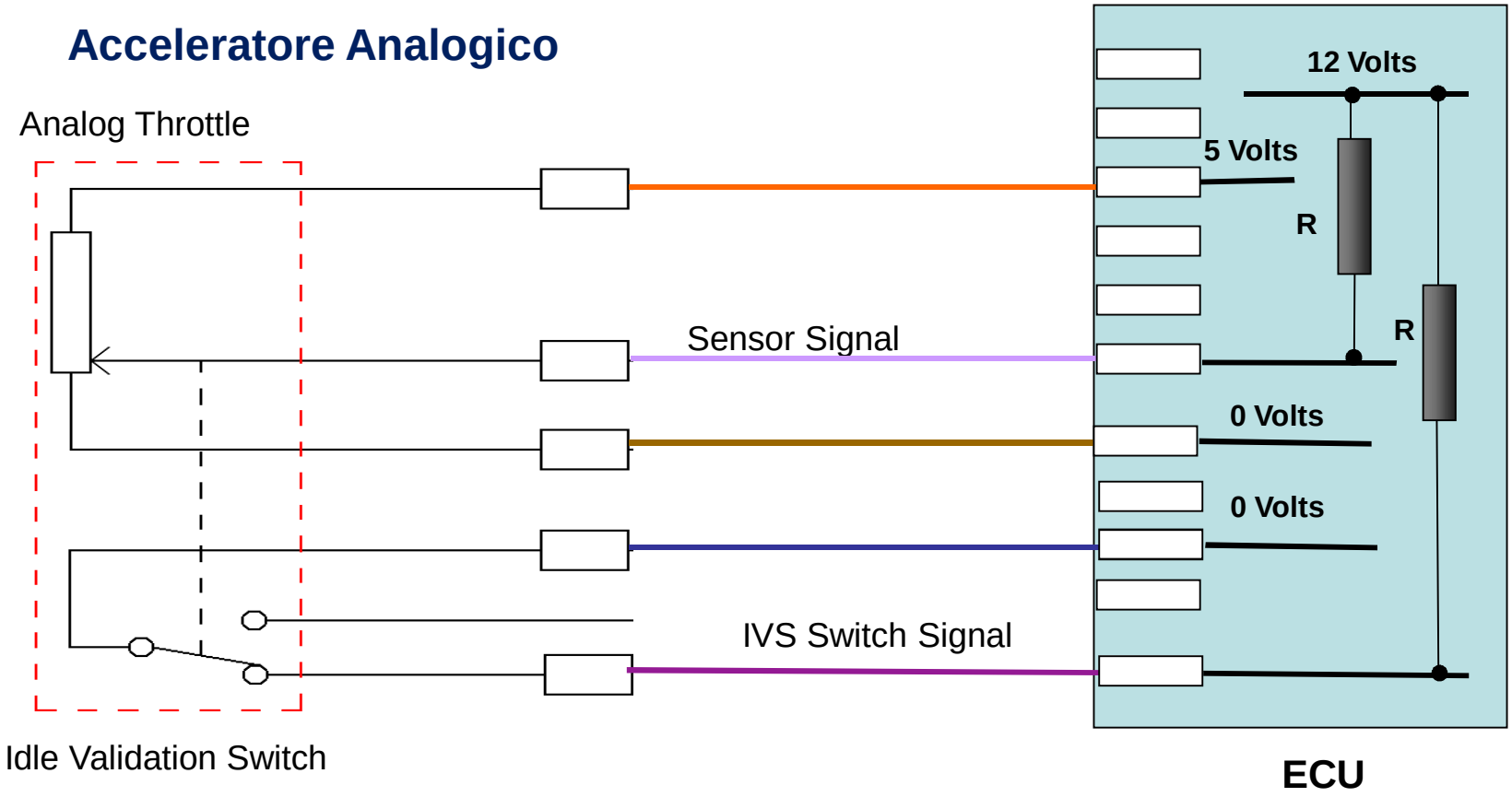
Il caso dei trasduttori che rendono in uscita 4 – 20 mA è il più evidente.



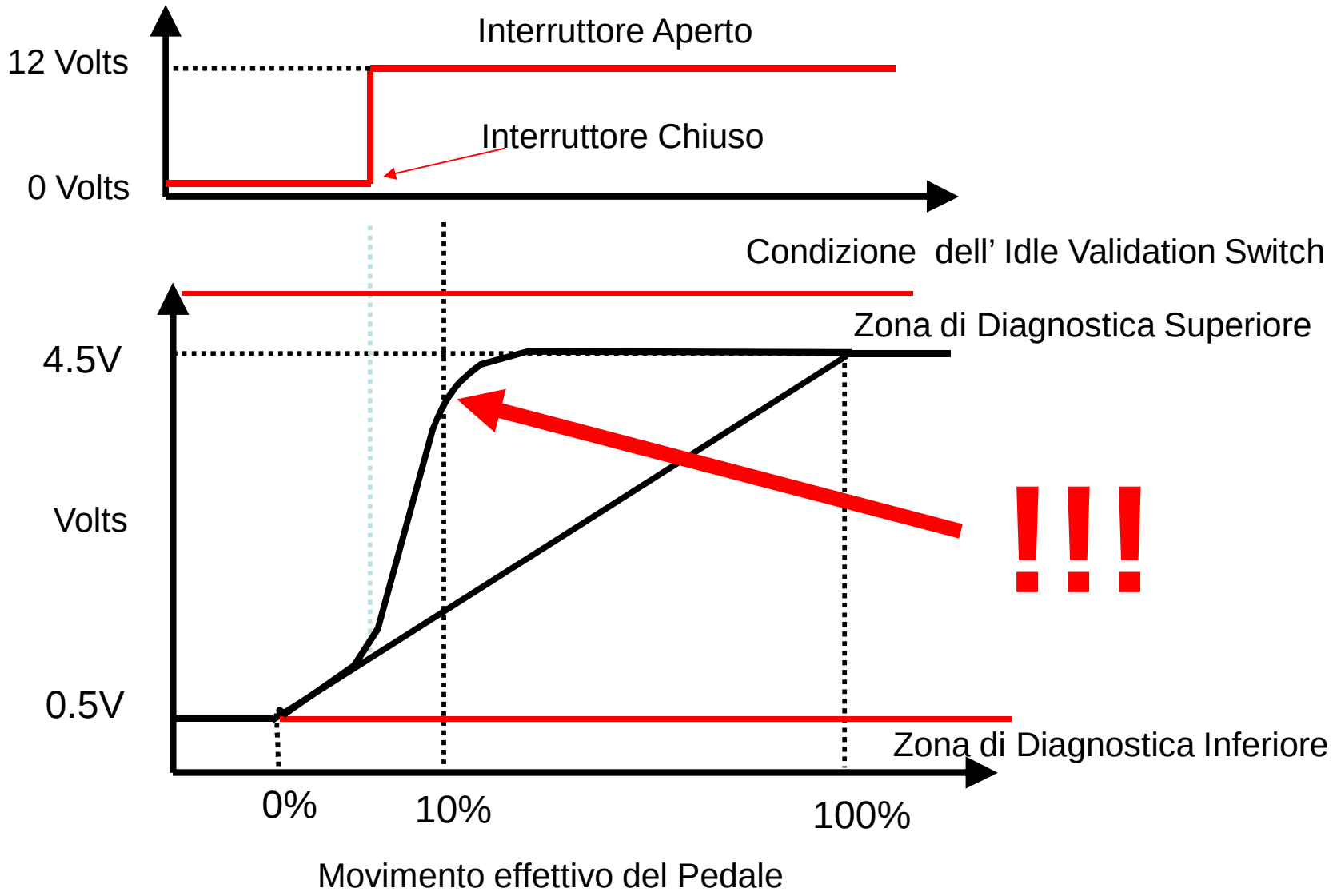
Alimentazione	Segnali in Uscita
5 Vdc Stabilizzati 12 ÷35 Vdc Non regolati 10 Vdc (max. tensione di alimentazione per sensori non condizionati)	0.5÷4.5 V Raziometrico 0÷5 V, 0÷10 V, 4÷20 mA. 2 mV/V per uscita non condizionata

Gestione delle ridondanze

Funzionamento di acceleratore analogico con Idle Position Validation Switch

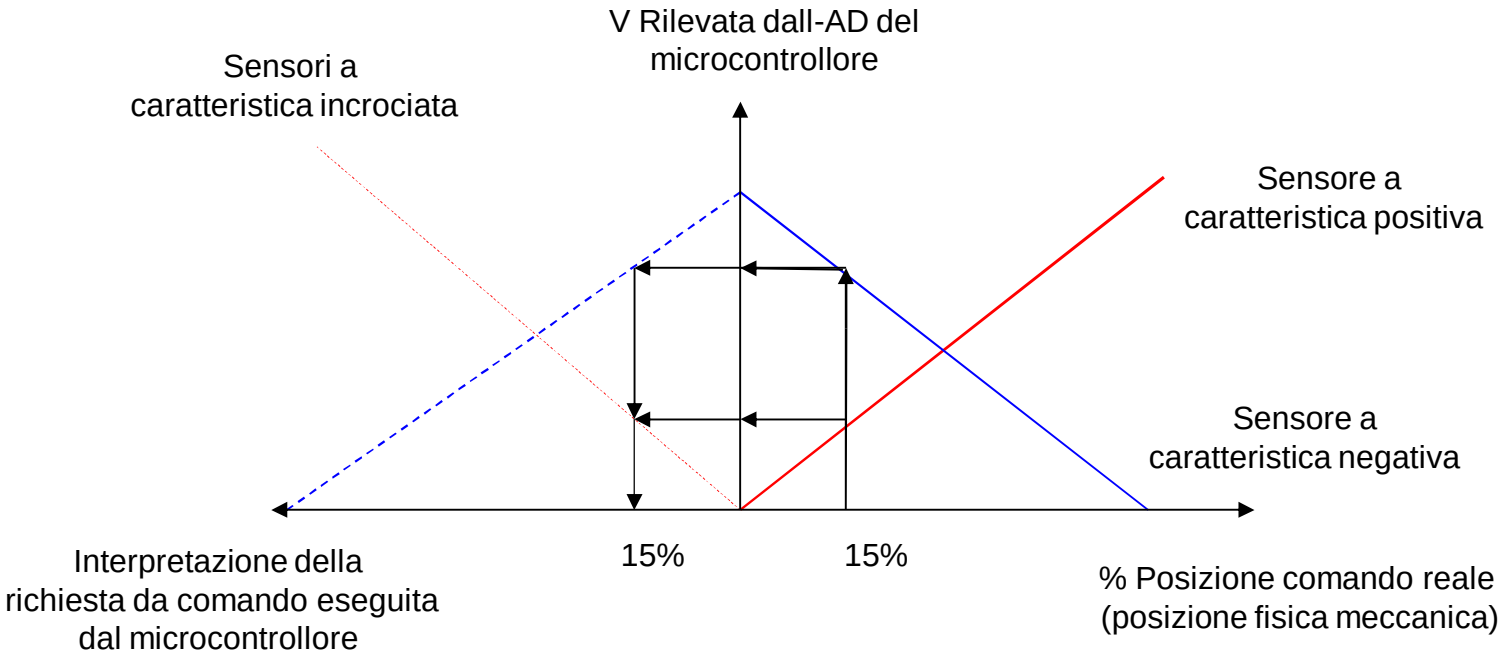


Gestione delle ridondanze



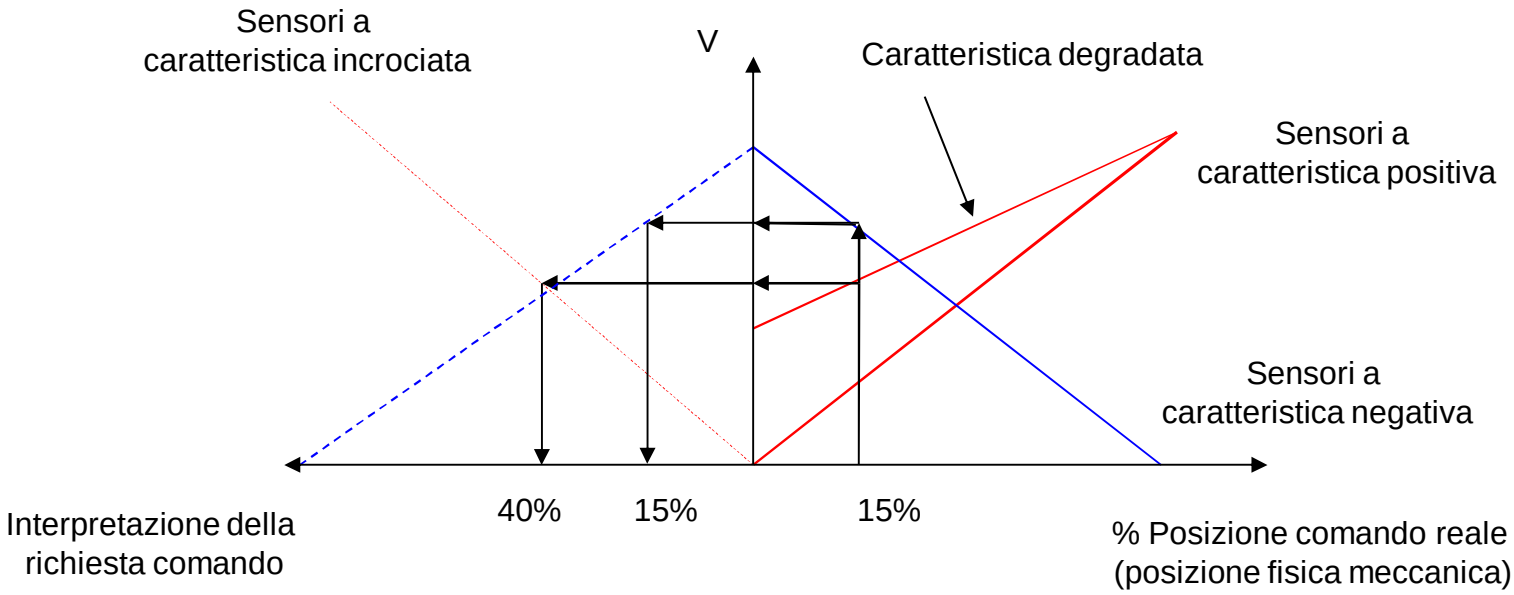
Gestione delle Ridondanze

Caratteristica del segnale del sensore di un comando



Gestione delle Ridondanze

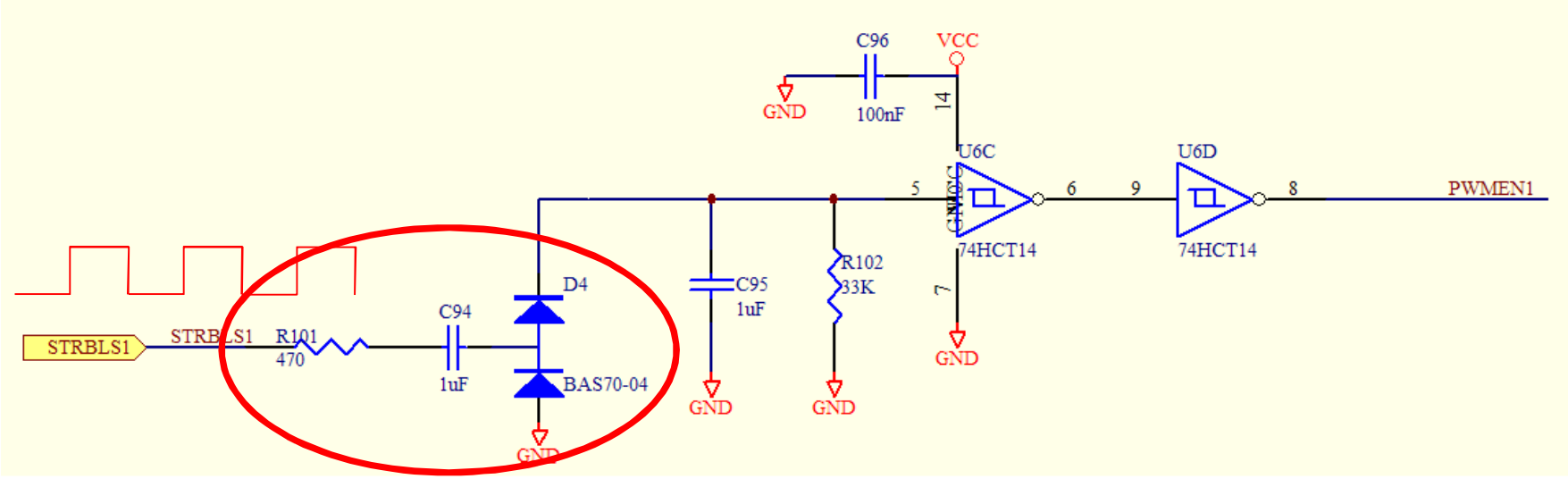
Caratteristica del segnale del sensore di un comando



Knowledge base nella progettazione safe

Sfruttare la *Diversity* nelle attuazioni

Soluzioni ad hoc sono state sintetizzate dalle diverse aziende, tra le più comuni l'utilizzo di dispositivi di controllo esterno per i microcontrollori (watch dog) e sicurezze hardware sui canali di abilitazione dei carichi elettrici di comando degli attuatori elettroidraulici. Per sfruttare la Diversity si consiglia di utilizzare tecniche diverse, in questo caso un filtro RC serie che mette in sicurezza gli attuatori anche in caso di blocco del microcontrollore.

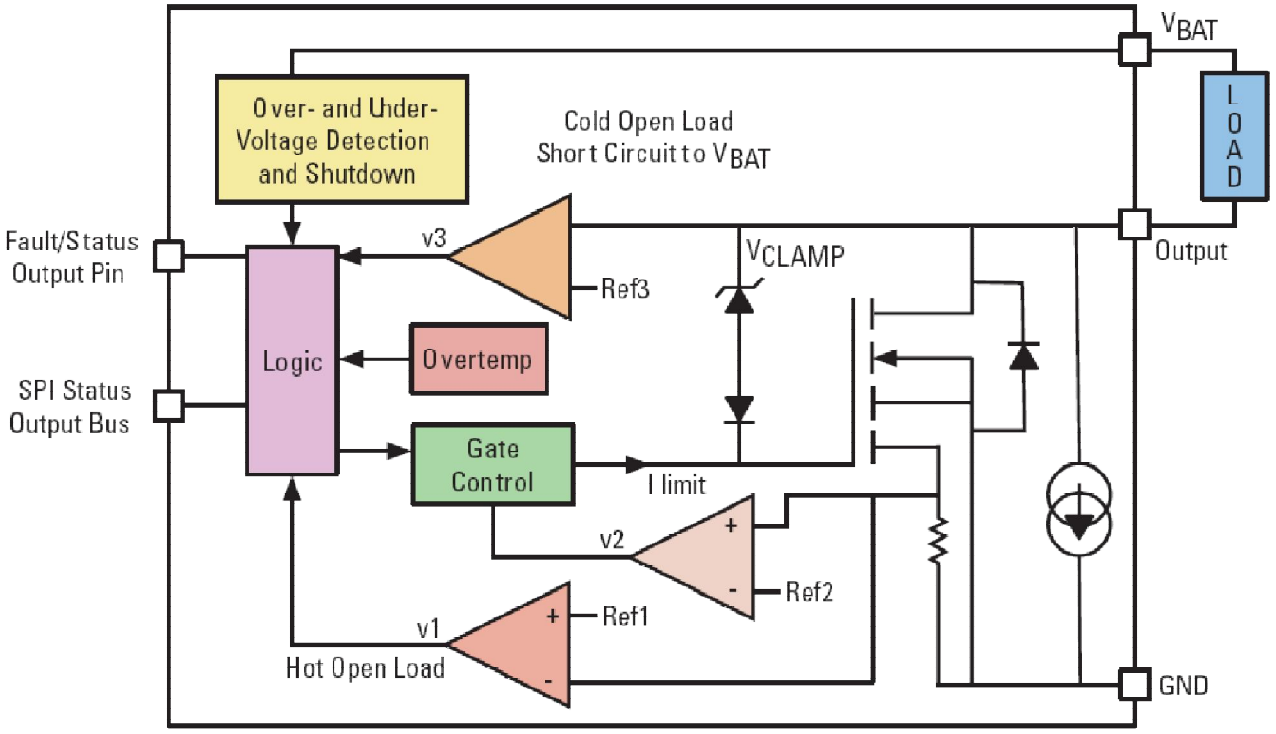


Trend nella progettazione elettronica

I maggiori costruttori di componentistica elettronica sono consapevoli delle variate necessità del mercato automotive e propongono componentistica elettronica sempre più vicina agli standard di sicurezza attiva in molti campi:

- Driver di potenza con capacità di autodiagnosi e caratteristiche elettriche sempre migliori: R_{dson} 10 volte inferiore a quella dei modelli dei 2001; è quindi possibile il collegamento di driver in serie per realizzare stadi di potenza ridondanti e quindi sicuri.

SmartMOS



Trend nella progettazione elettronica

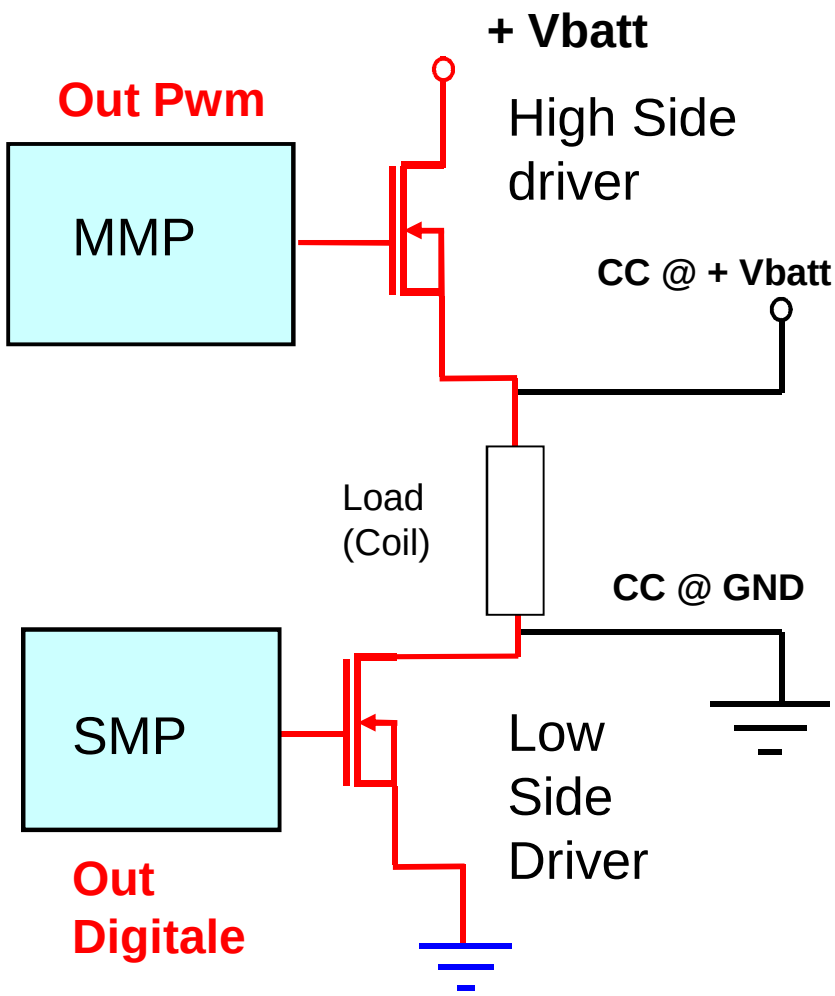
I maggiori costruttori di componentistica elettronica sono consapevoli delle variate necessità del mercato automotive e propongono componentistica elettronica sempre più vicina agli standard di sicurezza attiva in molti campi:

- Qualità nelle acquisizioni analogiche: design migliorato e qualità nell'isolamento del rumore e dei disturbi EMC, permette la lettura di cadute di tensione su resistenze di 100 μΩ.

- Consapevolezza della impossibilità di una analisi di sicurezza delle unità elettroniche che prescinda dallo studio della applicazione specifica

Ridondanza nel controllo delle attuazioni

Asymmetrical Half Bridge



La soluzione ottimale protegge sia da corti verso massa che da corti verso l'alimentazione.
In ogni caso si può interrompere il flusso della corrente lungo la linea di potenza, togliendo l'abilitazione ai driver di potenza.

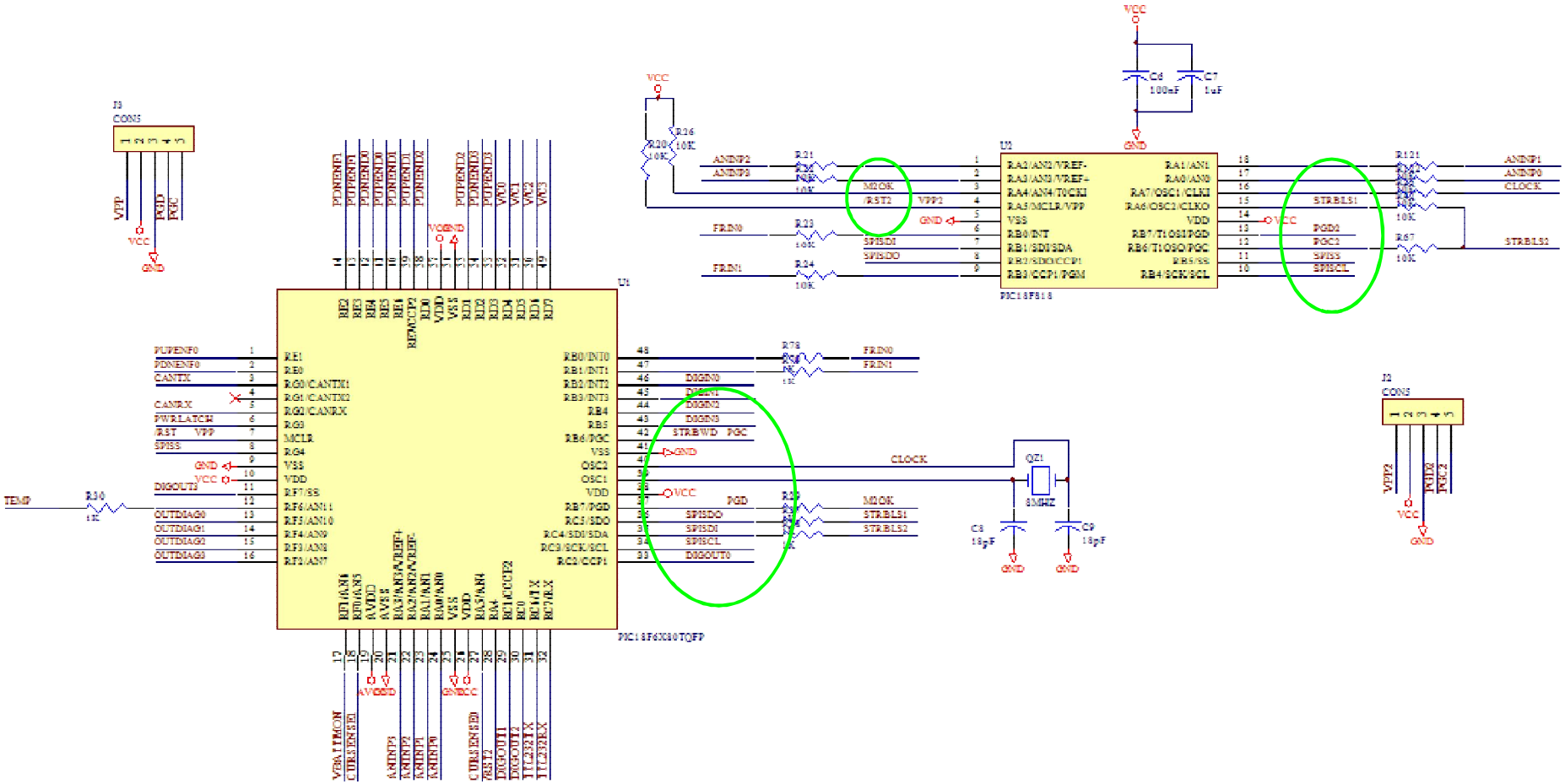
In caso in cui non si utilizzasse questa soluzione la valvola pilotata non sarebbe protetta dai corto circuiti e il sistema non potrebbe essere definito sicuro.

Lo svantaggio di questa soluzione rispetto a quella che utilizza un solo driver è che si perde un po' di differenza di potenziale ai capi del carico a causa della caduta di tensione ai capi dei driver, che in questo caso sono due.

Knowledge base nella progettazione safe

Redundancy nella struttura di calcolo

Si iniziano a progettare unità a due microcontrollori, con una vera e propria ridondanza sia a livello HW che di controllo delle principali grandezze acquisite.

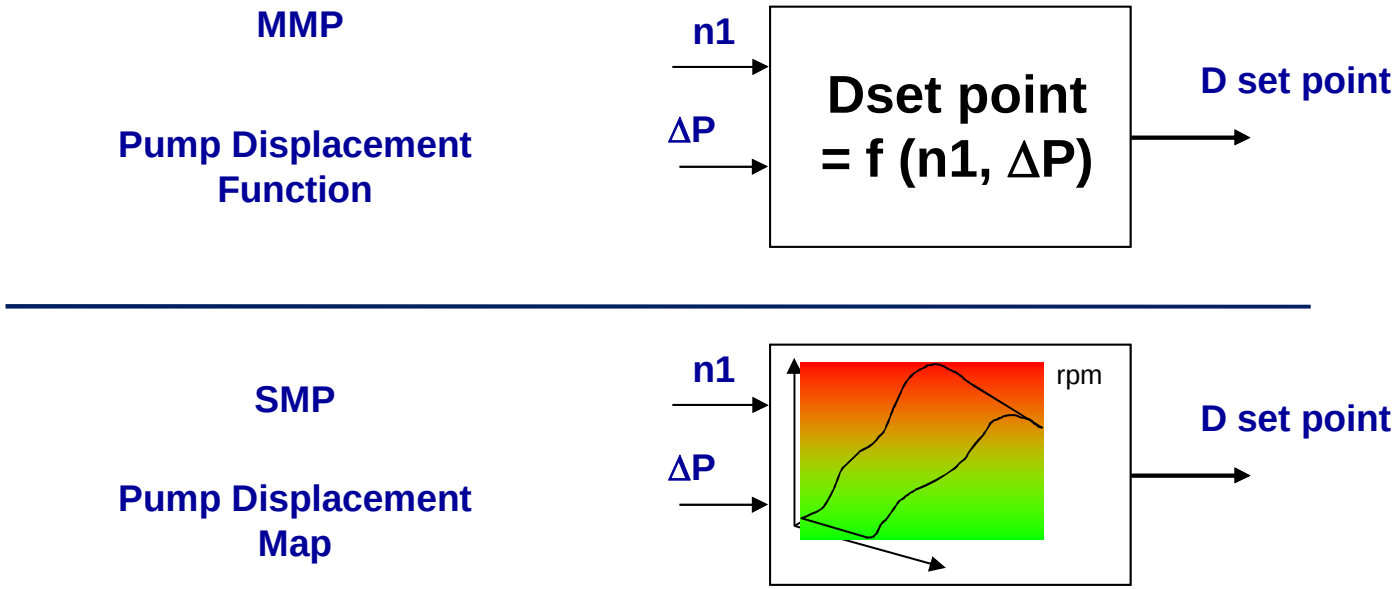


Knowledge base nella progettazione safe

Diversity nella struttura di calcolo

Le strategie di controllo vanno controllate dal sistema ridondante diversificando il metodo di calcolo, per evitare errori sistematici nel software o nelle strategie di controllo stesse.

Ad esempio una strategia può essere *model based* nel microcontrollore che esegue effettivamente l'attuazione e *mappata* nel supervisore.



Trend e Innovazione nella progettazione elettronica

Due sono le tendenze principali, uno che porta verso una grande flessibilità e potenza dei sistemi elettronici programmabili e uno che porta verso una maggiore sicurezza.

- I sistemi divengono componenti grazie alla sempre più spinta integrazione: IC Programmabili che integrano periferiche che erano precedentemente all'esterno dei microcontrollori

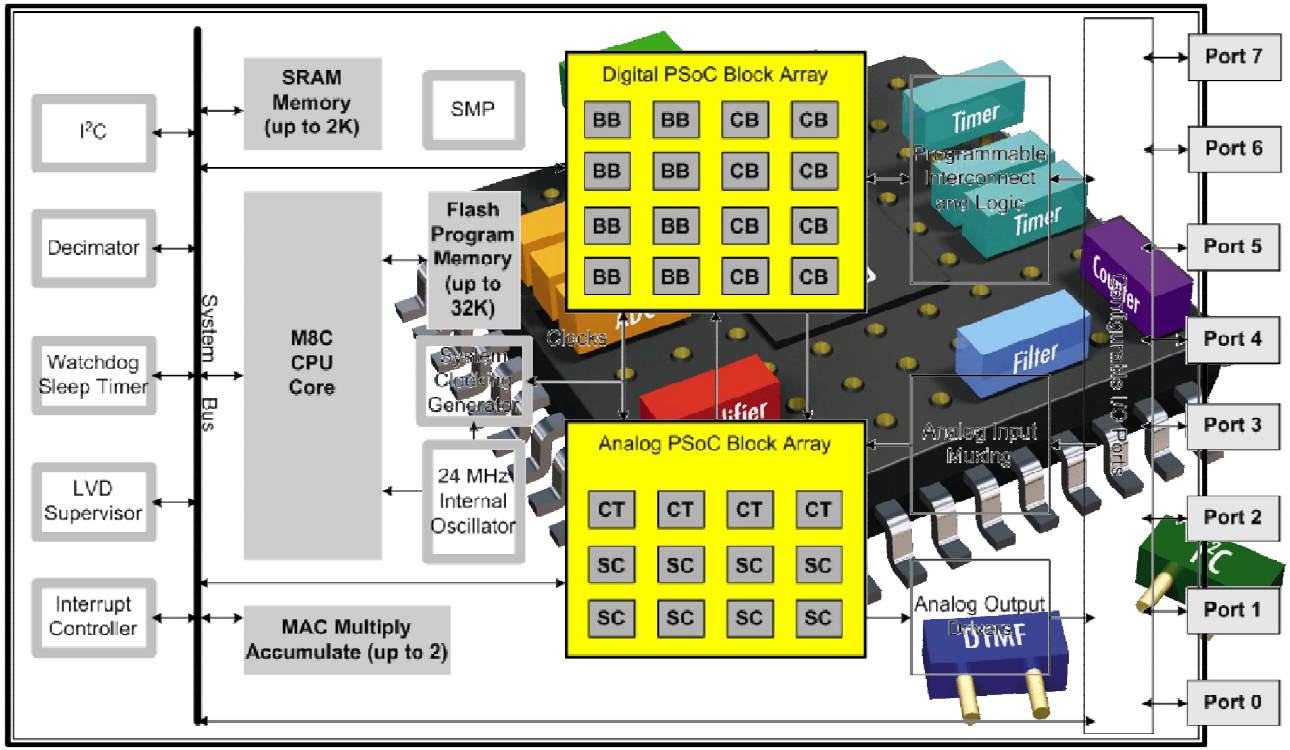
PSoC:

Programmable

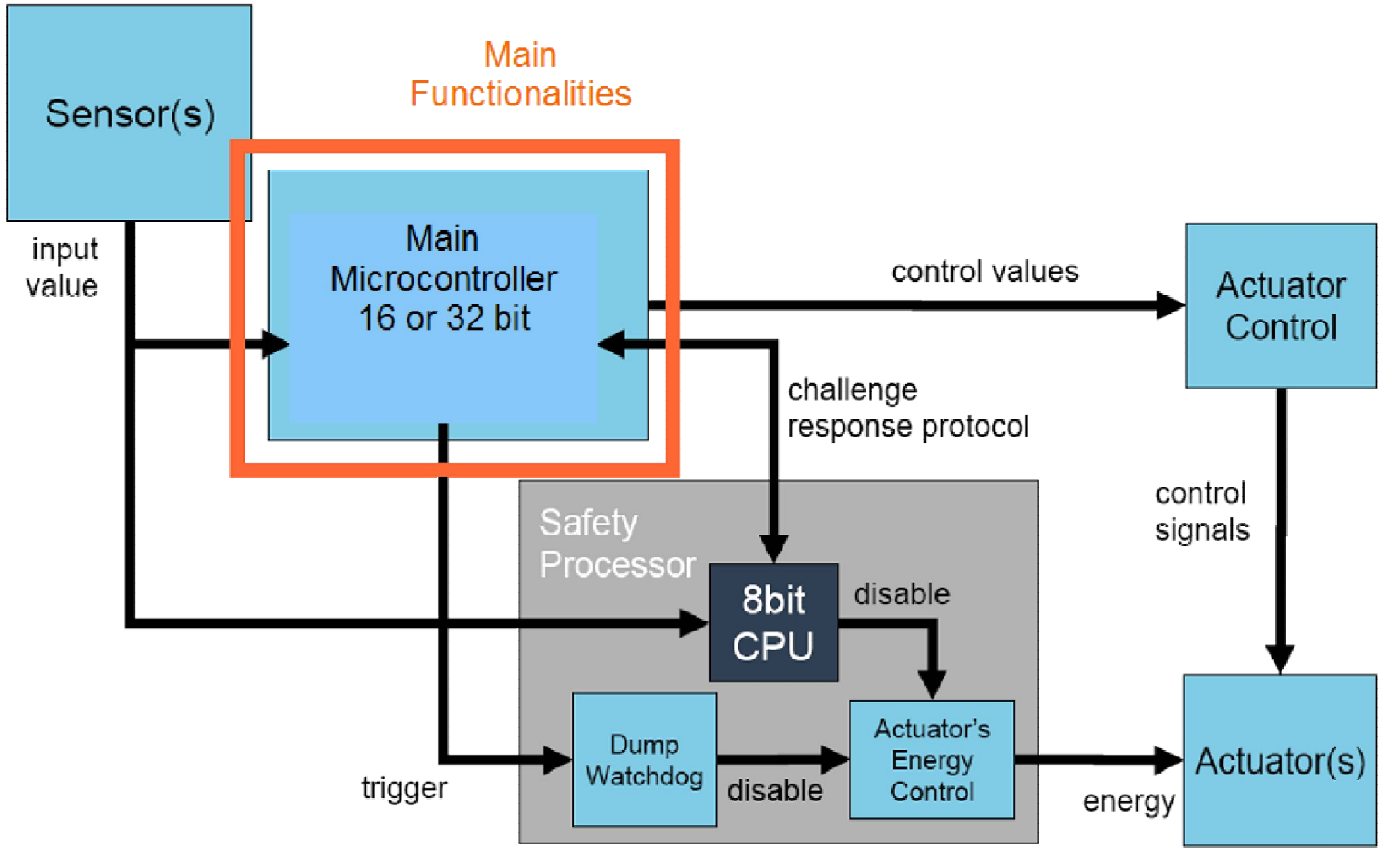
System

on

Chip

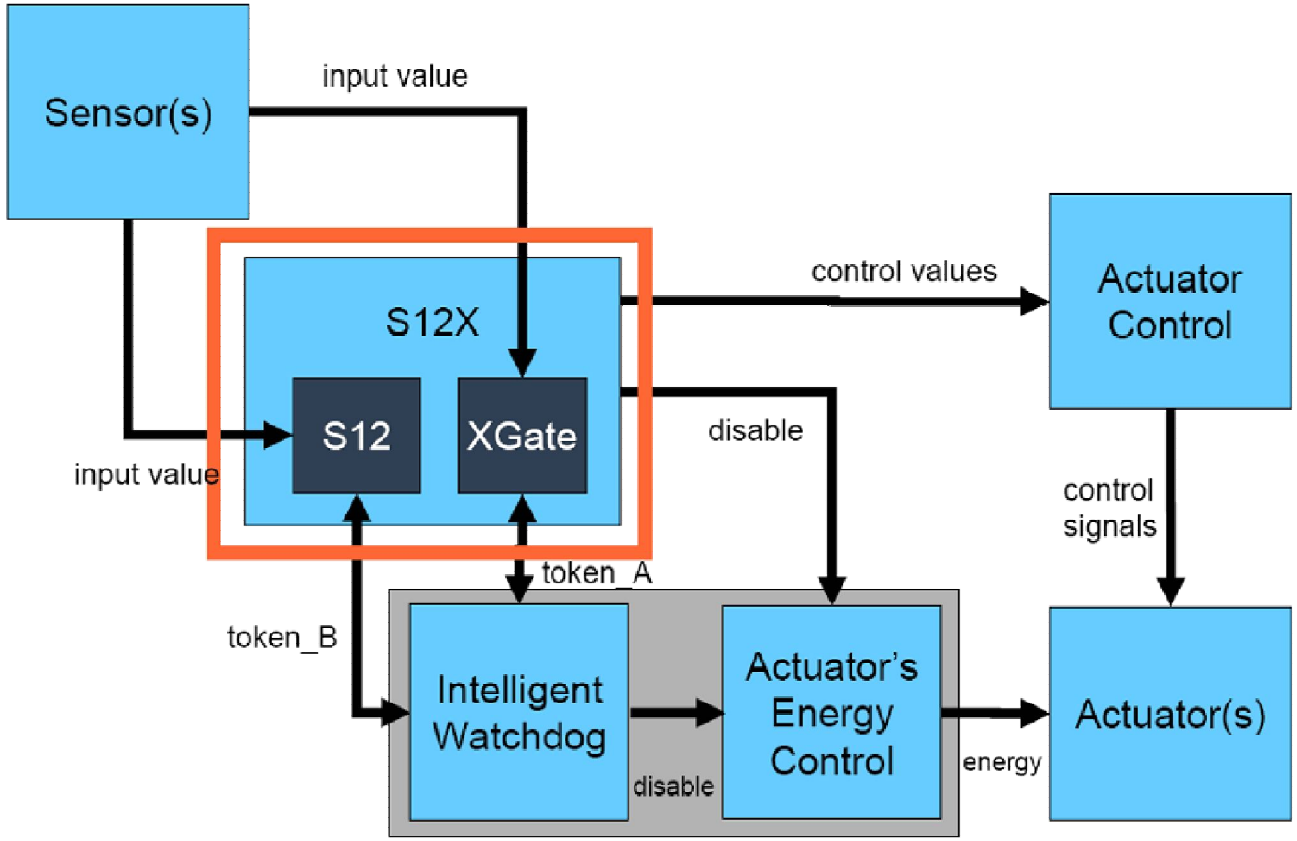


Microcontrollori: ridondanza tradizionale



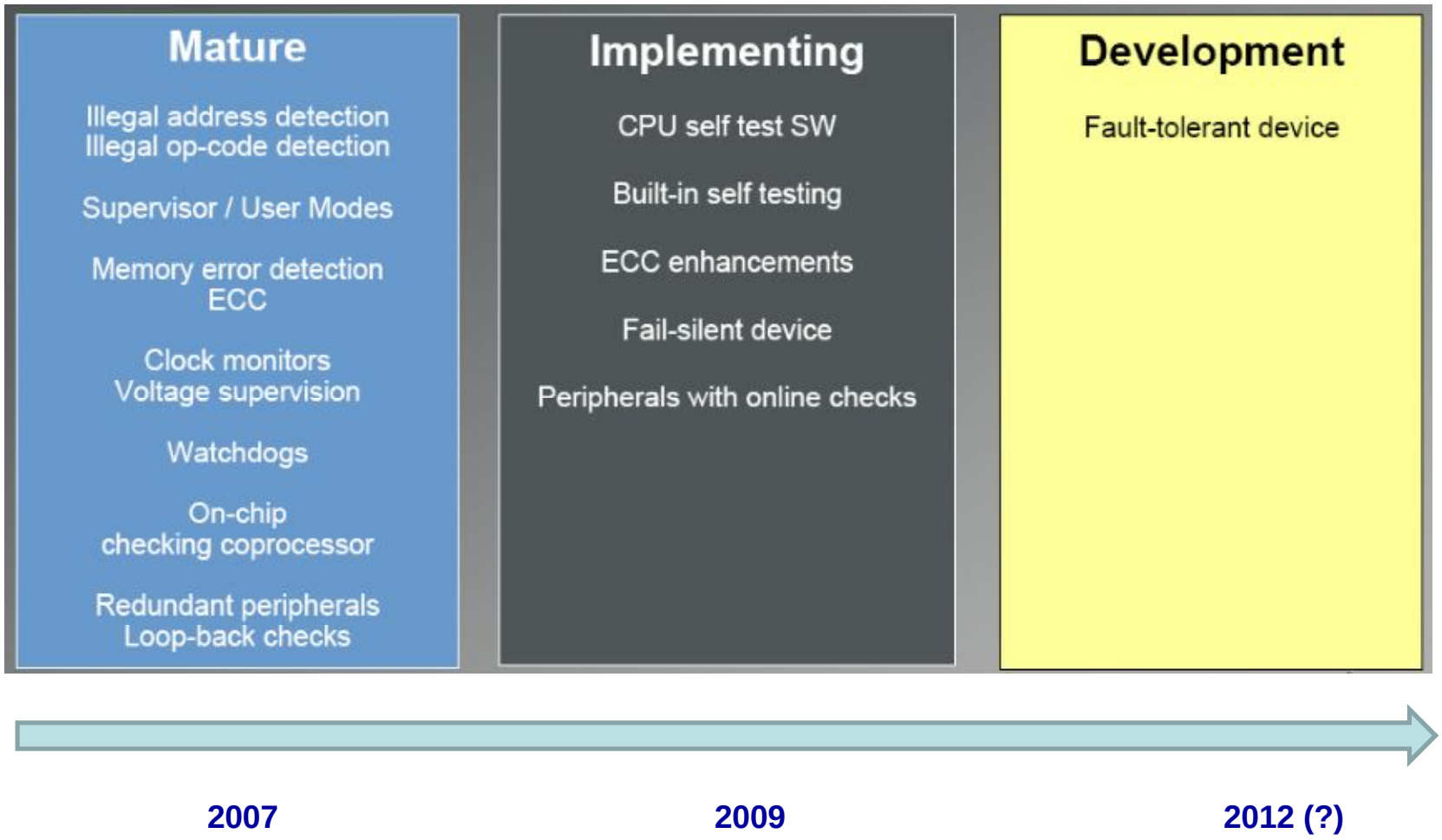
Layout di sistema tradizionale per la realizzazione di sistema con ridondanza Funzionale a doppio microcontrollore

Microcontrollori Multicore



Layout di sistema innovativo per la realizzazione di sistema con ridondanza funzionale a singolo microcontrollore con X-Gate di Freescale Semiconductor: Design semplificato, minor consumo di potenza elettrica, minori problemi EMC, minor costo delle unità di controllo.

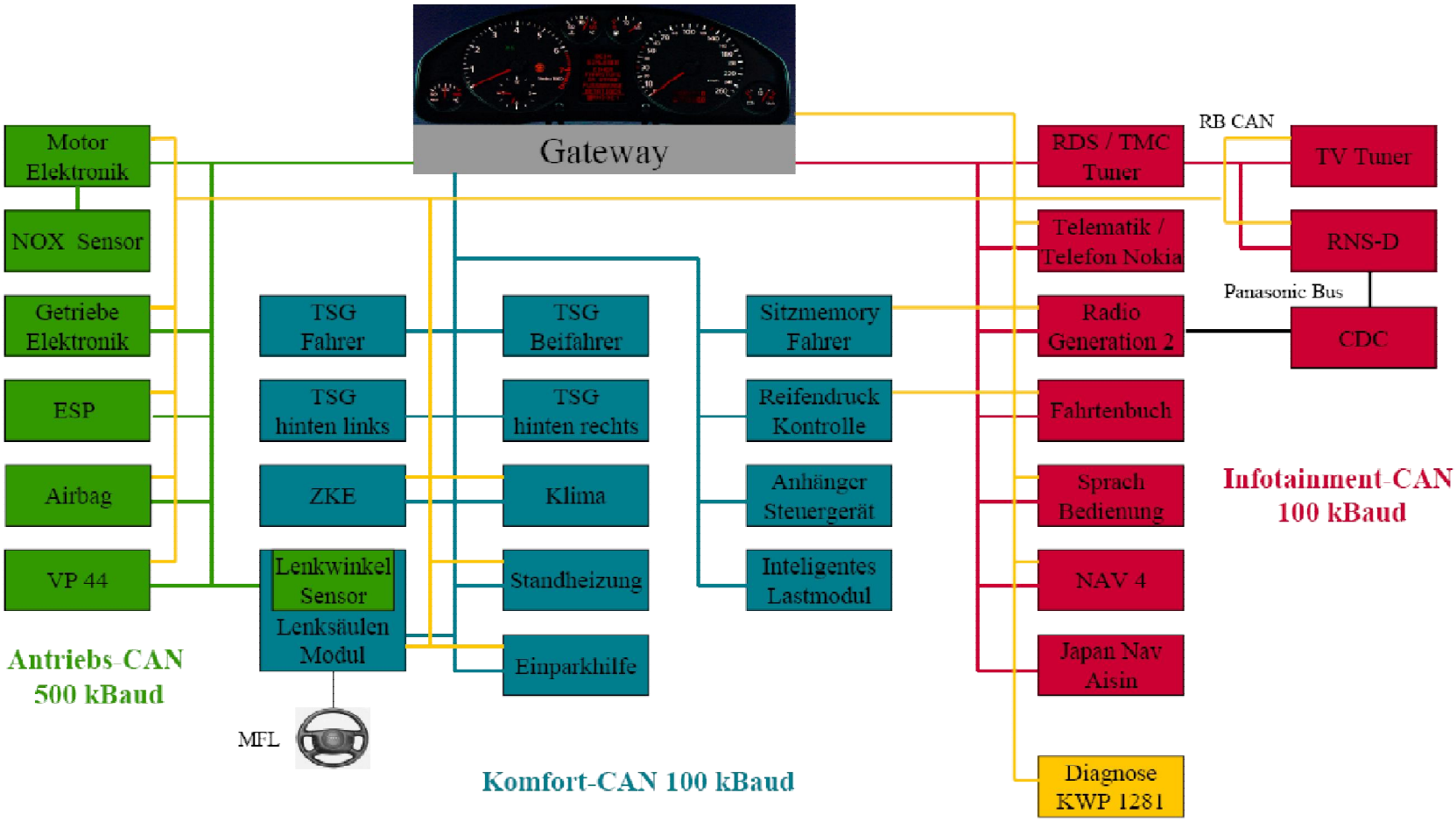
Microcontrollori



Alcune regole che riteniamo valide

- Uso di sistemi ridondanti in cui è ridonata anche la parte di alimentazione (regolatore di tensione) al fine di eliminare una CCF.
- Uso di Watch dog esterno per non essere dipendenti da un guasto della distribuzione della alimentazione del clock o della tensione all'interno dei microcontrollori.
- Uso di sistemi di comunicazione sincrona tra I micro per la verifica delle tempistiche e sincronizzazione delle operazioni.
- Uso di diversity sia nel calcolo delle funzioni di controllo sia nel trasferimento informativo
- Uso di paramteri e calibrazioni e file di aggiornamento criptati con chiavi asimmetriche per avere un elevato livello di sicurezza nella registrazione dei valori in memoria non volatile nei controllori.
- Uso di checksum e antichecksum locali ad aree ricontrollati a ogni power on su tutte le memorie del sistema.

Reti e Controllo distribuito

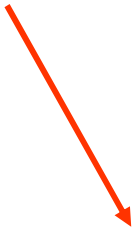


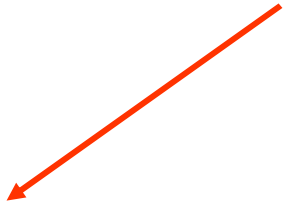
- CAN Network: le reti CAN sono divenute uno standard nella progettazione sistemistica degli autoveicoli ed è ormai avvenuto lo stesso anche per le macchine agricole e movimento terra, si pone il problema del controllo distribuito

Problemi legati alle reti CAN

- Massima velocità di trasmissione 1Mb/s
- In caso di elevata velocità di trasmissione della rete, limitata lunghezza massima della rete (riferimenti in ISO 11898)
- Massimo numero di unità elettroniche connettibili alla rete (< 30)
- Tempo di risposta della rete non deterministico: il ritardo del task di rete non è predicibile e dipende dalla priorità relativa dei messaggi in rete e dal carico di rete.
- Topologia fissa e piana della rete (non è possibile creare reti a stella, *repeaters*) : questo ingenera problemi di safety; molti brevetti sono stati depositati per tentare di aumentare il basso livello di sicurezza legato alla struttura delle reti CAN.
- Il *payload* massimo contenuto in un singolo messaggio è molto limitato (max 8 bytes): necessità dei cosiddetti *Transport protocol*.
- Problemi ineliminabili di "*message falsification*" dovuti alla tipica struttura del livello fisico e dei controlli hardware eseguiti dai CAN controller

Il CAN è adatto alla applicazione in Safety Related Systems?





LIFE SUPPORT APPLICATIONS

These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Philips customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Philips for any damages resulting from such improper use or sale.

BARE DIE DISCLAIMER

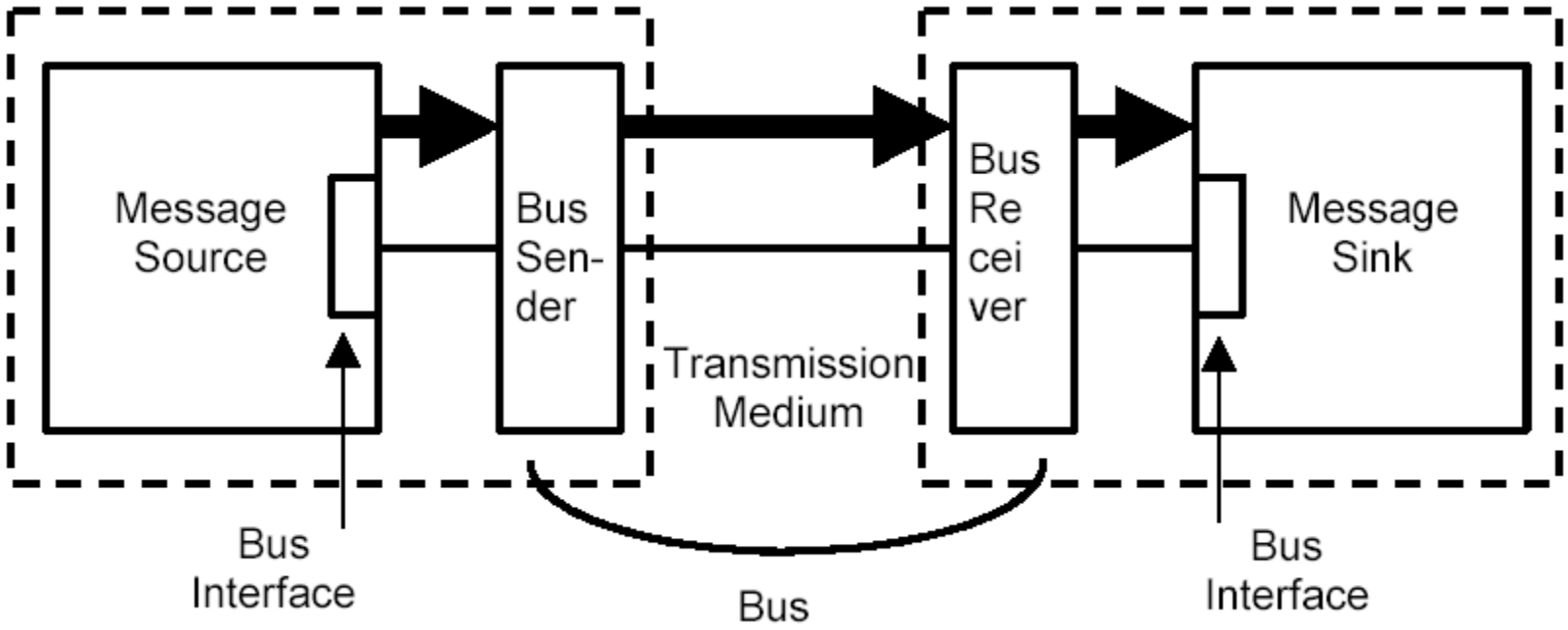
All die are tested and are guaranteed to comply with all data sheet limits up to the point of wafer sawing for a period of ninety (90) days from the date of Philips' delivery. If there are data sheet limits not guaranteed, these will be separately indicated in the data sheet. There are no post packing tests performed on individual die or wafer. Philips Semiconductors has no control of third party procedures in the sawing, handling, packing or assembly of the die. Accordingly, Philips Semiconductors assumes no liability for device functionality or performance of the die or systems after third party sawing, handling, packing or assembly of the die. It is the responsibility of the customer to test and qualify their application in which the die is used.

Raccomandazioni ISO 15998 sulle reti (CAN)

L’esperienza ha fatto proliferare soluzioni e brevetti per tentare di aumentare il livello di sicurezza delle reti CAN, sia a livello di layout di rete sia a livello di consistenza dei dati e la norma ISO15998 fornisce una serie di metodi applicativi per aumentare il livello di sicurezza della rete CAN.

Teoricamente La probabilità residua di errore su CAN è dell’ordine di 10^{-9}. tuttavia test affidabili hanno stabilito un 10^{-7} più prudenziale, che però va rapportato al numero di messaggi effettivamente scambiati nell’unità di tempo. Che porta il CAN a un valore prossimo a 10^{-4}. Non viene quindi raggiunto neppure il valore SIL2.

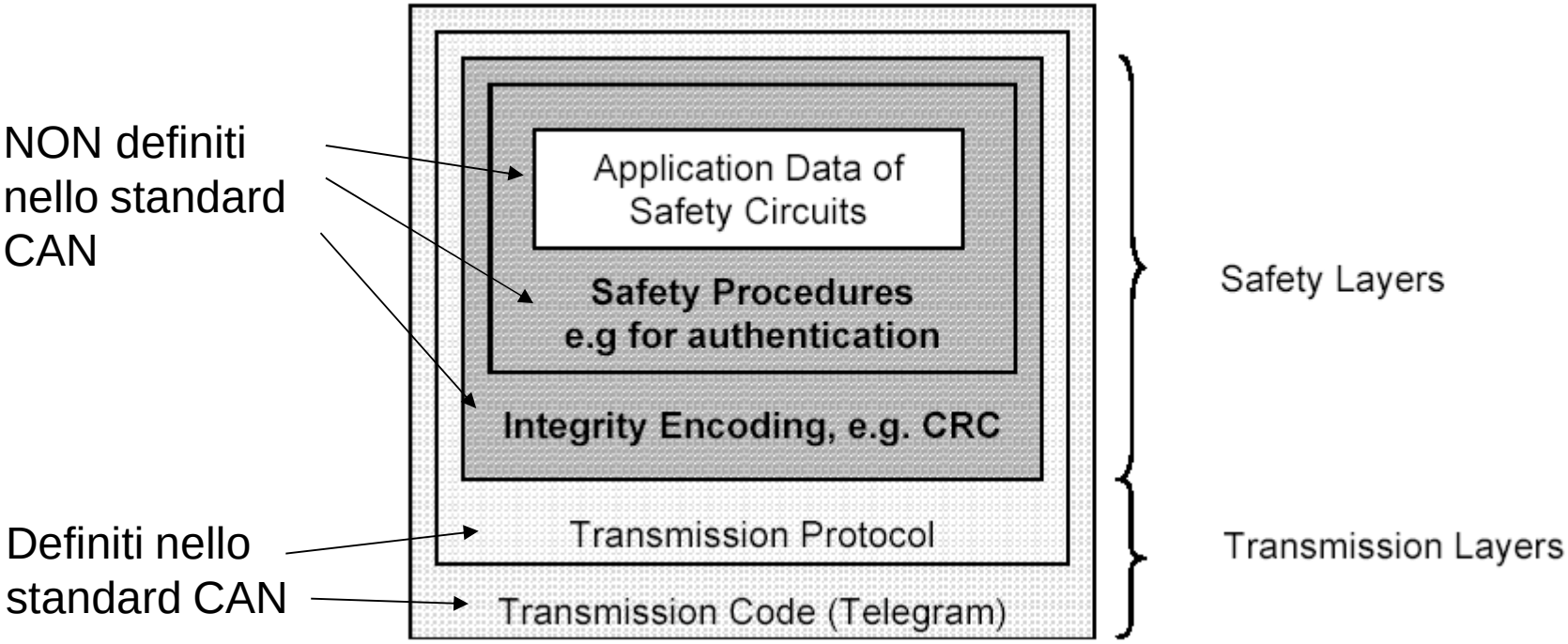
Trasmissione di messaggi safety-related su bus di comunicazione



Un sistema a bus di comunicazione è identificato da sorgente e ricevitore dei messaggi, da un bus (medium/path) di comunicazione e dalle interfacce verso il bus, costituite dai controller/transceivers, protocollo ecc…

Struttura di un bus system con caratteristiche di sicurezza, su rete esistente

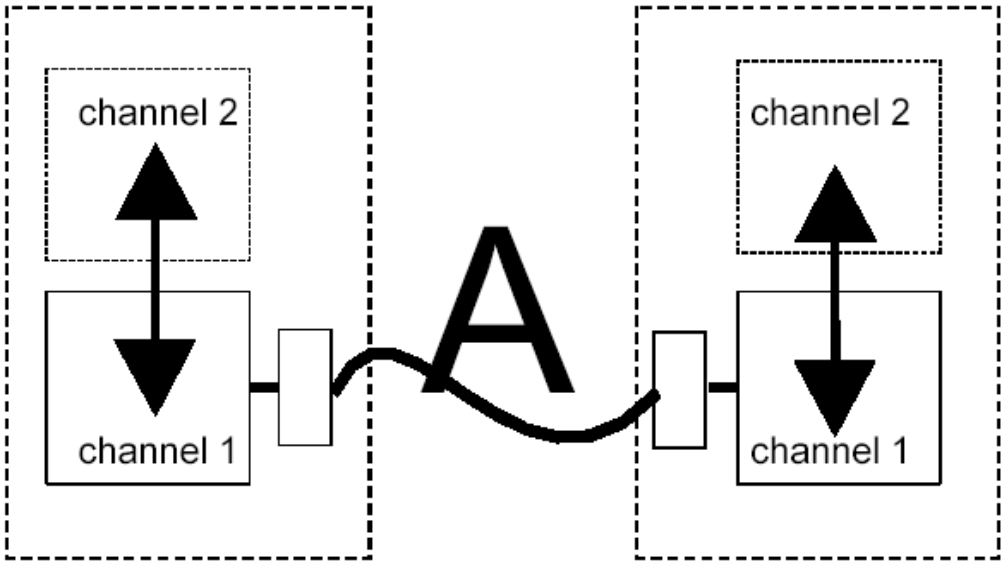
UN bus di comunicazione già esistente in commercio può essere reso sicuro, anche se non “fault tolerant”, agendo sul solo supporto software aggiunto alla gestione della comunicazione a basso livello.



Struttura di un bus system (2)

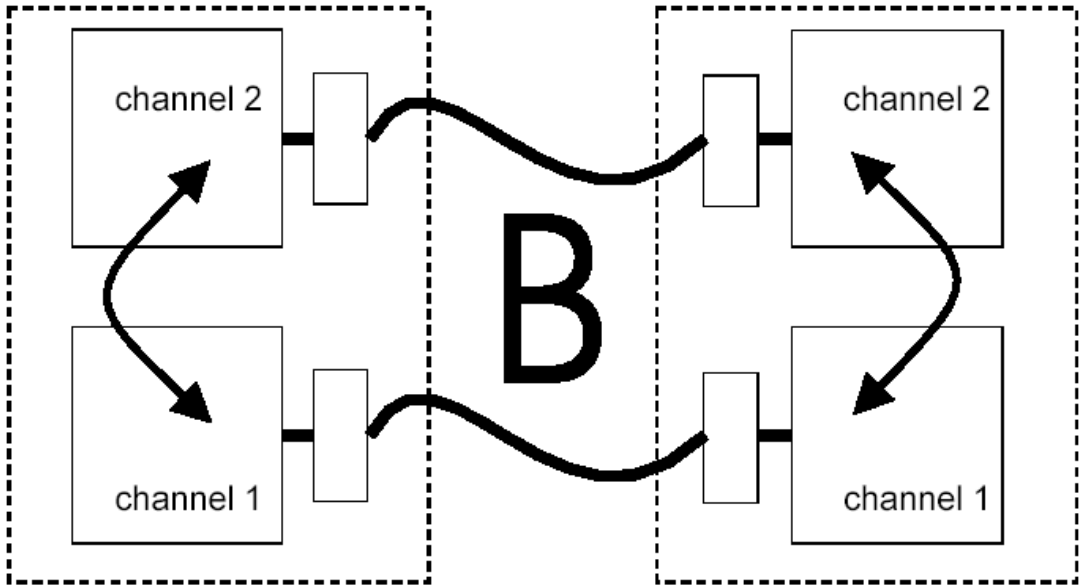
Nello schema riportato nella slide precedente, si riconosce la strutturazione della norma ISO-OSI per i sistemi di comunicazione.
Le novità riguardano non le definizioni, ma le restrizioni d'uso dei sistemi a bus nei veicoli.
Un "encapsulated bus system" è costituito da un numero fissato o massimo fissato o predeterminato di unità afferenti che sono connesse tra di loro mediante uno o più mezzi trasmissivi e seguendo determinate performance e caratteristiche di trasmissione

Architetture possibili (1)



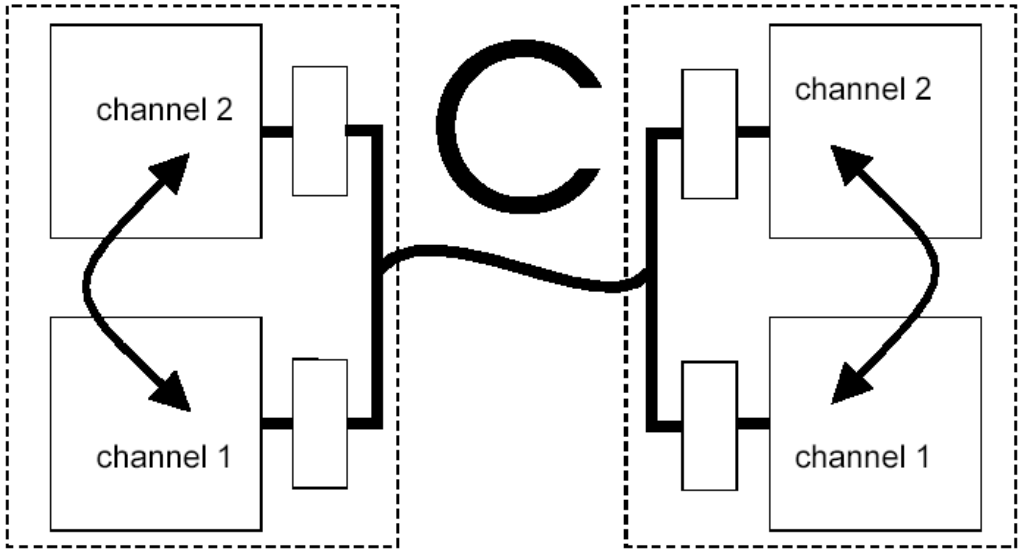
A: Struttura a singolo canale trasmissivo, priva di ridondanza e con una solo interfaccia al bus per ogni coppia di “channel”, i messaggi propri dei canali 2 sono passati ai canali 1 prima di poter essere trasmessi sul bus.
Qui gli user data possono essere trasmessi in uno o due messaggi per ogni unità.

Architetture possibili (2)



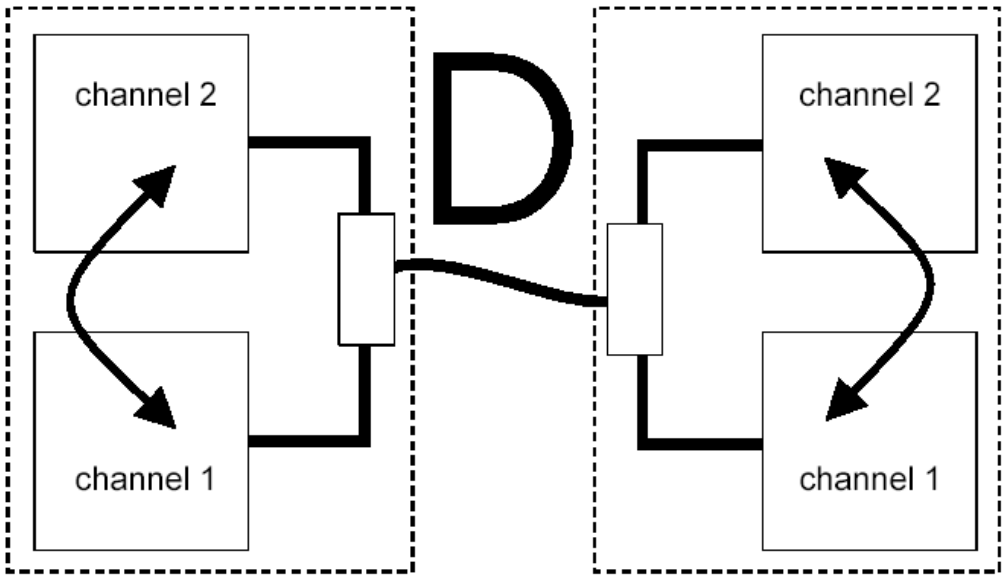
B: Struttura a doppio canale trasmissivo, ridondante e con due interfacce al bus per ogni coppia di “channel”, uno per ogni canale. Tutti i safety layer e i transmission layer sono doppi.
Qui gli user data vengono trasmessi in due messaggi per ogni unità.

Architetture possibili (3)



C: Struttura a singolo canale trasmissivo, ridondante nelle interfacce al bus, una per ogni “channel”, uno per ogni canale. Tutti i safety layer e i transmission layer sono doppi. Ma non il transmission media.
Un solo mezzo trasmissivo.
Qui gli user data vengono trasmessi in due messaggi per ogni unità.

Architetture possibili (4)



D: Struttura a singolo canale trasmissivo, non ridondante nelle interfacce al bus, una per ogni coppia di “channel”. I *safety layer* sono raddoppiati ma non i *transmission layer*. Ogni safety Layer ha un accesso indipendente al canale trasmissivo.
Qui gli user data possono essere trasmessi in uno o due messaggi per ogni unità.

Definizioni per la trattazione degli errori

Vengono identificate alcune definizioni utili alla enunciazione dei principi di sicurezza per i sistemi in rete:

- **Maximum extension size:** massimo numero di sorgenti e ricevitori dei messaggi
- **Process safety time**: è il periodo di tempo che intercorre tra il verificarsi di un fault e il verificarsi di una situazione di rischio se non vengono prese contromisure di sicurezza
- **Electrical reaction time**: è il tempo tra il riconoscimento elettrico dell'evento safety-related e l'inizio della reazione elettrica della strategia di sicurezza.

Tipologie di errori di trasmissione (1)

- **Repetition**: a causa di un errore in una delle unità afferenti alla rete uno dei messaggi è ripetuto con dati vecchi, non aggiornati, è ripetuto ad un istante di tempo non corretto (vecchio).

- **Loss**: Un messaggio è distrutto a causa di un fault in una delle unità della rete

- **Insertion**: un messaggio viene inserito a causa di un errore in uno dei partecipanti alla rete

- **Incorrect sequence**: La corretta sequenza dei messaggi viene alterata a causa di un errore in uno dei partecipanti

Tipologie di errori di trasmissione (2)

- **Message falsification**: un messaggio viene alterato a causa di errori nei partecipanti o nel mezzo trasmissivo

- **Retardation**: una safety function viene ritardata o addirittura impedita a causa di overload di traffico di messaggi non-safety-related

- **Coupling of safety related and non safety related messages**: messaggi safety-related e non-safety-related vengono trattati allo stesso modo e confusi a causa di errori in una unità afferente al bus.

Misure per il controllo degli errori di trasmissione (1)

- **Running number**: numero progressivo di messaggio scambiato tra sender e receiver
- **Time Tag**: Tempo trasmesso assieme al messaggio e relativo alla validità del messaggio; si possono specificare alcuni diversi Time Tag:
  - **Relative Time Tag**: tempo derivato da un local clock del sender
  - **Absolute Time Tag**: tag derivato da un global time scambiato tra loro dalle unità afferenti alla rete
  - **Dual Time Tag**: tag scambiato tra due unità che mettono in relazione I loro time locali, una sorta di sincronizzazione che tiene conto del tempo assoluto dell'altra unità, senza modificare il proprio local time

Misure per il controllo degli errori di trasmissione (2)

- **Time Expectation (time-out)**: tempo Massimo che può intercorrere tra due messaggi di un certo tipo scambiati tra due unità

- **Reception Acknowledgement**: messaggio inviato in ritorno ad un messaggio ricevuto, che dia la possibilità al sender del messaggio originario di capire se il messaggio originario è stato ricevuto correttamente dal ricevente

- **Identification for Message sender and receiver**: informazioni contenute nel messaggio che identifichino il sender e i receiver (destinatari) del messaggio stesso

Misure per il controllo degli errori di trasmissione (3)

- **Redundancy with cross monitoring**: in strutture come B e C ogni messaggio è trasmesso due volte da ciascun channel e inoltre viene eseguito un check tra le due unità trasmittenti e le due riceventi per valutare la correttezza del messaggio inviato

- **Different Data Integrity assurance safety-related (SR) and non-safety-related (NSR) data**: diverse metodologie di valutazione della correttezza dei messaggi vengono utilizzate per SR e NSR data, per evitare influenze spurie dei messaggi NSR sugli SR.

Misure per evitare errori di trasmissione

La norma parte dall'assunto che il solo mezzo trasmissivo (bus + transceivers) non possa essere considerato sufficientemente sicuro per garantire la trasmissione corretta dei messaggi. La responsabilità della sicurezza dei messaggi è esclusivamente delle unità trasmittenti e riceventi.

Una serie di regole guida di base devono quindi essere seguite dai progettisti al fine di avere maggiori certezze relativamente ai messaggi ricevuti e inviati:

- E' necessario utilizzare un meccanismo di time expectation (time-out).
- Un sistema di riconoscimento degli errori di trasmissione deve essere implementato nelle unità riceventi, in grado di attivare safety-related reaction in caso di transmission failure entro il massimo tempo di reazione identificato.

Misure per evitare errori di trasmissione (2)

- In caso di errori di trasmissione si deve attivare l'opportuna error reaction.
- Non si deve mai eccedere il tempo massimo di reazione (process safety time) specificato dal costruttore anche in caso di fault.
- Per la trasmissione dei safety-related messages debbono essere effettuate tutte le misure per assicurare che ogni tipo di errore sia riconosciuto entro i process safety time prestabiliti.
- I sistemi non-safety-related messages non devono influenzare i tempi di trasmissione/ricezione dei sistemi safety-related.

Definizione di frequenza di errore residua

La maggior parte delle reti in commercio presenta già integrati nel protocollo o addirittura direttamente in hardware (come nel caso del CAN) alcuni controlli di errore, per la verifica della integrità del dato trasmesso e ricevuto.
In una rete come la rete CAN, la probabilità di rilevare un errore singolo presente in un messaggio ricevuto è molto alta, così come è alta la probabilità di rilevare un errore doppio, le probabilità di rilevare errori multipli si riducono esponenzialmente all'aumentare del numero di errori.

La probabilità residua di errore è la probabilità di NON rilevare la presenza di un errore, quando invece questo sia effettivamente presente.

Tutto questo indipendentemente dalla capacità di correggere l'errore rilevato, ovvero non si ha la pretesa di correggere l'errore, ma solo di rilevarlo, al fine di non processare dati affetti da errori.

Parallelamente la frequenza di errore residua è il numero di errori non rilevati nell'unità di tempo.

Data integrity assurance method

La garanzia della integrità dei dati è fondamentale per il raggiungimento del safety integrity level stabilito in fase di progetto.
E' fornita una formula per il calcolo della *frequenza di errore residua* Λ sulla base della probabilità di errore residua R(p):

$$\Lambda = 3600 \cdot R(p) \cdot \nu \cdot m \cdot 100$$ [errori di trasmissione/ora]

ove 3600 sono i secondi in un'ora, v è frequenza richiesta [1/s] dei safety related message per ottenere il tempo di reazione desiderato, R(p) è la probabilità residua di errore e m è il numero di messaggi necessario per realizzare la *safety-related function*. Il 100 che moltiplica il numero è il fattore di scala che riporta la probabilità di errore in termini percentuali.
Per la stima di R(p) ci si deve basare sulle caratteristiche dei sistemi dichiarate dai costruttori, e la probabilità di errore di bit va calcolata come p=0,01 in assenza di altre informazioni.

Data integrity assurance method (2)

Sono definiti 3 livelli di Safety Integrità Level (SIL) secondo quanto definito dalla norma IEC61508:

$$SIL3 \rightarrow \Lambda \leq 10^{-7}$$

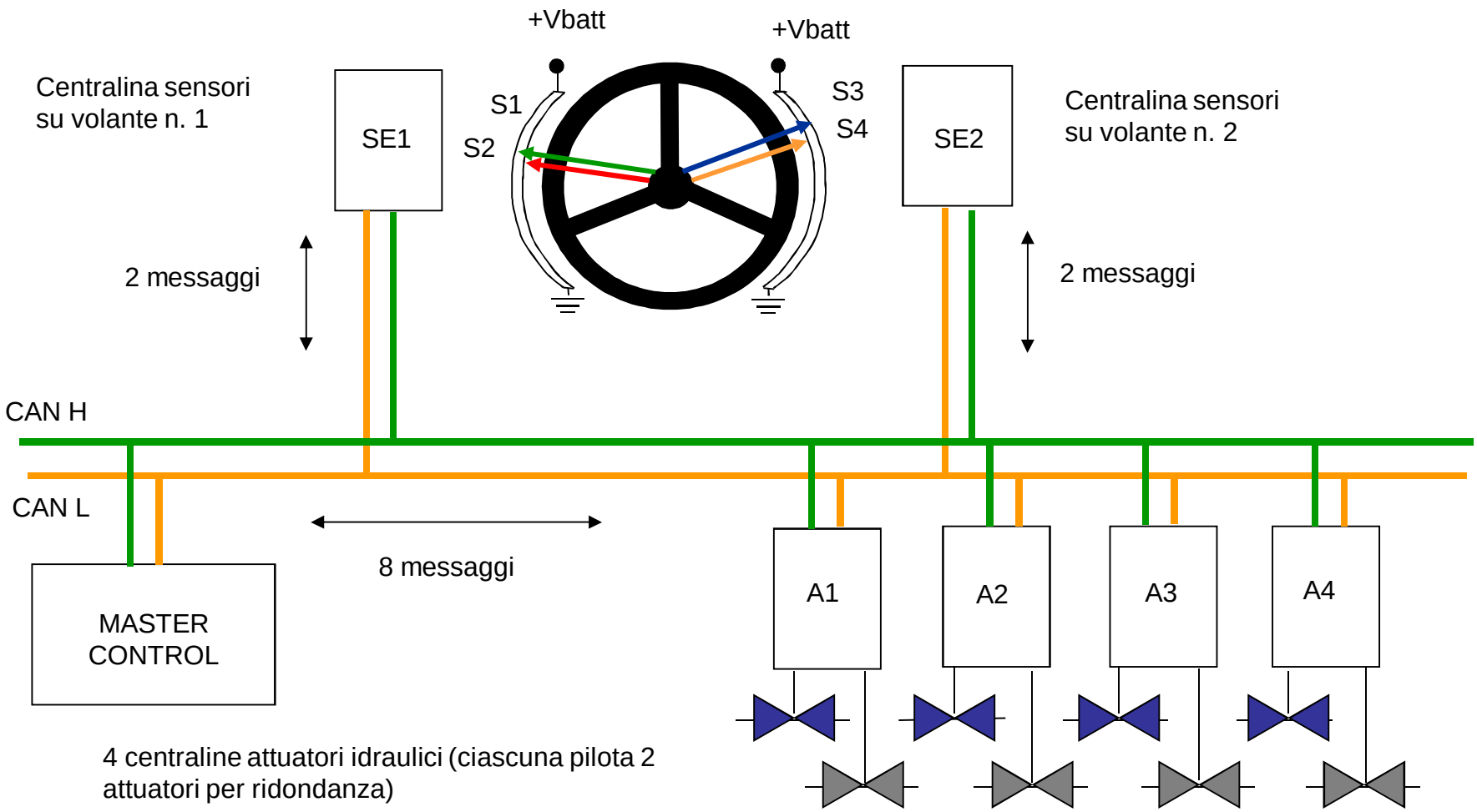
$$SIL2 \rightarrow \Lambda \leq 10^{-6}$$

$$SIL1 \rightarrow \Lambda \leq 10^{-5}$$

In termini assolutamente generici, si può affermare che una applicazione che risponda alla specifica di sicurezza soddisfacendo la soglia SIL2 può ritenersi sicura, se si tratta di una applicazione di tipo automotive.

Un esempio di ciò che significhino tali livelli può aiutare a individuare gli ordini di grandezza del problema.

Esempio: Steering by Wire Elettroidraulico



4 centraline attuatori idraulici (ciascuna pilota 2 attuatori per ridondanza)

Esempio: Steering by Wire (2)

Il sistema di controllo del sistema di sterzatura Steering by wire di un veicolo ha la movimentazione del volante sensorizzato controllata da due sensori potenziometrici a due piste parallele ciascuno (pista 1 e 2 a sinistra del volante e pista 3 e 4 a destra). Si richiede il SIL 2.

Si noti che per il mero funzionamento sarebbe sufficiente la lettura di un solo sensore potenziometrico da parte di una centralina, ma per ridondanza funzionale si predispongono 2 sensori doppi acquisiti in modo indipendente da due unità elettroniche.

Il master control riceve i valori dei 4 potenziometri sul volante e, dopo avere controllato la congruenza dei valori dei potenziometri, elabora le strategie di sterzatura e le trasmette a 4 unità di calcolo che comandano 8 attuatori elettroidraulici.

Si suppone 1 messaggio (*bus telegram*) per ogni asse e uno per ogni attuatore, quindi 2+2+8 messaggi nella rete.

Esempio: Steering by Wire (3)

Altro dato fondamentale di progetto è la frequenza di messaggio minima che consente il rispetto dei tempi massimi di reazione in caso di guasto: 100 ms, allora una frequenza di 10 messaggi/s. allora v è = 10 [1/s]. Il *worst case* R(p) = $7x10^{-9}$

Si suppone che un errore riconosciuto sia segnalato sulla rete attraverso error frames.

Tutto ciò che è errore non riconosciuto è invece oggetto del calcolo di sicurezza.

Per la frequenza residua di errore il calcolo diviene:

$$\Lambda = 3600 \cdot R(p) \cdot v \cdot m \cdot 100 = 3600 \cdot 7 \cdot 10^{-9} \cdot 10 \cdot 12 \cdot 100$$

che risulta pari a 0,3024 > 10^{-6}. Quindi il sistema non soddisfa le specifiche e non è SIL 2 (ma neppure SIL 1), il sistema non è sicuro.

Qualche precisazione sull’esempio

Da notare il fatto che, nella formula, all’aumentare del numero di messaggi si ha un aumento del Λ.

Allo stesso modo anche all’aumentare della frequenza minima dei messaggi si ha un aumento del Λ.

Tutto ciò che porta un aumento del traffico sulla rete nell’unità di tempo, porta anche un aumento delle probabilità che vi sia un messaggio errato (aumentano infatti i messaggi) non riconosciuto come tale. Aumenta quindi la probabilità residua di errore.

Va anche notato che in presenza di una rete con probabilità residua di errore specifica molto bassa, il Λ si mantiene basso anche in presenza di elevati traffici sulla rete stessa.

Come riportare il sistema nelle specifiche
(ovvero come aumentarne il grado di sicurezza)

Il sistema non è sicuro per l'elevato numero di messaggi, la probabilità residua abbastanza alta nel worst case, e una frequenza minima di messaggio non trascurabile.

Per aumentarne il livello di sicurezza si può aumentare il livello di sicurezza della trasmissione di ogni singola informazione safety-related: ogni messaggio diviene costituito da 2 *bus telegrams,* la cui consistenza viene controllata dalle unità riceventi e, in caso di inconsistenza dei dati, sarà intrapresa una immediata reazione di sicurezza.

Inviando le informazioni due volte, un errore identico dovrebbe essere commesso entrambe le volte per non riconoscere un errore in trasmissione.

Come riportare il sistema nelle specifiche (2)
(ovvero come aumentarne il grado di sicurezza)

La probabilità di una “falsification” del messaggio in questo caso è determinata dalla probabilità nel worst case, che risulta il prodotto delle probabilità residua dei worst case singoli già visti nel caso precedente: $R(p)xR(p)=7*7*10^{-9}*10^{-9}=49*10^{-18}$.

Il calcolo della frequenza di errore residua diviene:

$$\Lambda = 3600 \cdot R(p)^2 \cdot \nu \cdot m \cdot 100 = 3600 \cdot 49 \cdot 10^{-18} \cdot 10 \cdot 12 \cdot 100 = 0{,}002 \cdot 10^{-6} \leq 10^{-6}$$

che soddisfa la disuguaglianza del SIL 2, come richiesto dal progetto.

Elenco dei possibili errori di trasmissione e delle relative misure correttive

Errore di Trasmissione	Running Number	Time Tag	Time Expectation	Reception Acknowledgement	Identification for sender & receiver	Data Integrity Assurance	data Redundancy with cross check	Different Data integrity Assurance for SR & NSR
Repetition	X	X					X	
Loss	X			X			X	
Insertion	X			X	X		X	
Incorrect sequence	X	X					X	

Elenco dei possibili errori di trasmissione e delle relative misure correttive (2)

Errore di Trasmissione	Running Number	Time Tag	Time Expectation	Reception Acknowledgement	Identification for sender & receiver	Data Integrity Assurance	Redundancy with cross check	Different Data integrity Assurance for SR & NSR data
Message falsification				X		X	X	
Retardation		X	X					
Coupling of SR & NSR messages				X	X			X

Misure per il controllo degli errori nelle reti

Si dimostra che utilizzando per ogni informazione *safety relevant*:

1. Running Number
2. Time Expectation (Timeout)
3. Software CRC nei messaggi
4. Explicit Acknowledgement

La comunicazione CAN diventa sicura, e si è in grado di riportare il sistema in condizioni di *Fail Silent* in caso di presenza di errori nella rete.

Esempio:
AntiSkid Bosch in applicazioni Automotive

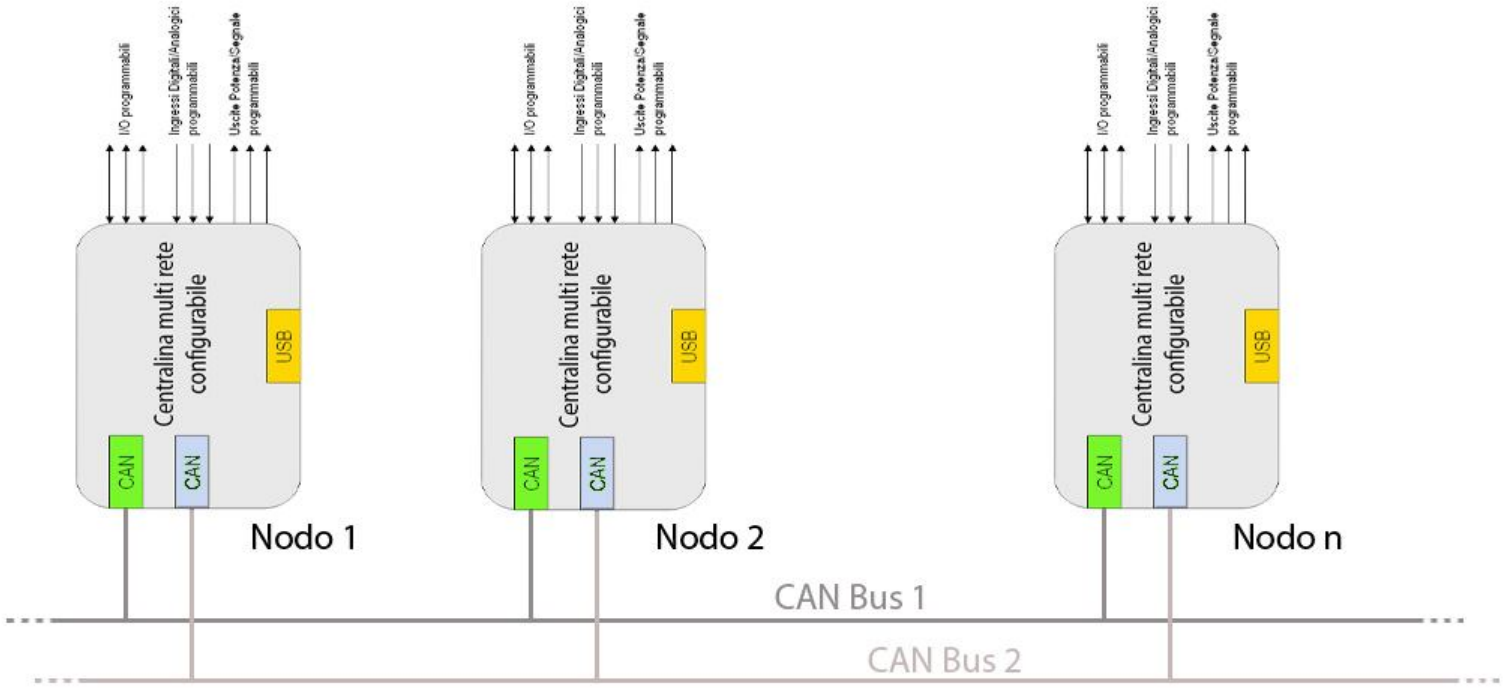
Richiesta di riduzione percentuale di coppia dall'ASR al Controllo Motore, messaggio inviato ogni 4 ms (esempio richiesta riduzione coppia del 30% e numero di messaggio 20).

Running Number	Percent Torque Reduction Request (MSB)	Percent Torque Reduction Request (LSB)	Negate of Percent Torque Reduction Request (MSB) - Running Number	Negate of Percent Torque Reduction Request (LSB)
N	%TRMSB	%TRLSB	~(%TRMSB) - N	~(%TRLSB)
0x14	0x01	0x2C	0xFE-0x14	0xD3
0x14	0x01	0x2C	0xEA	0xD3

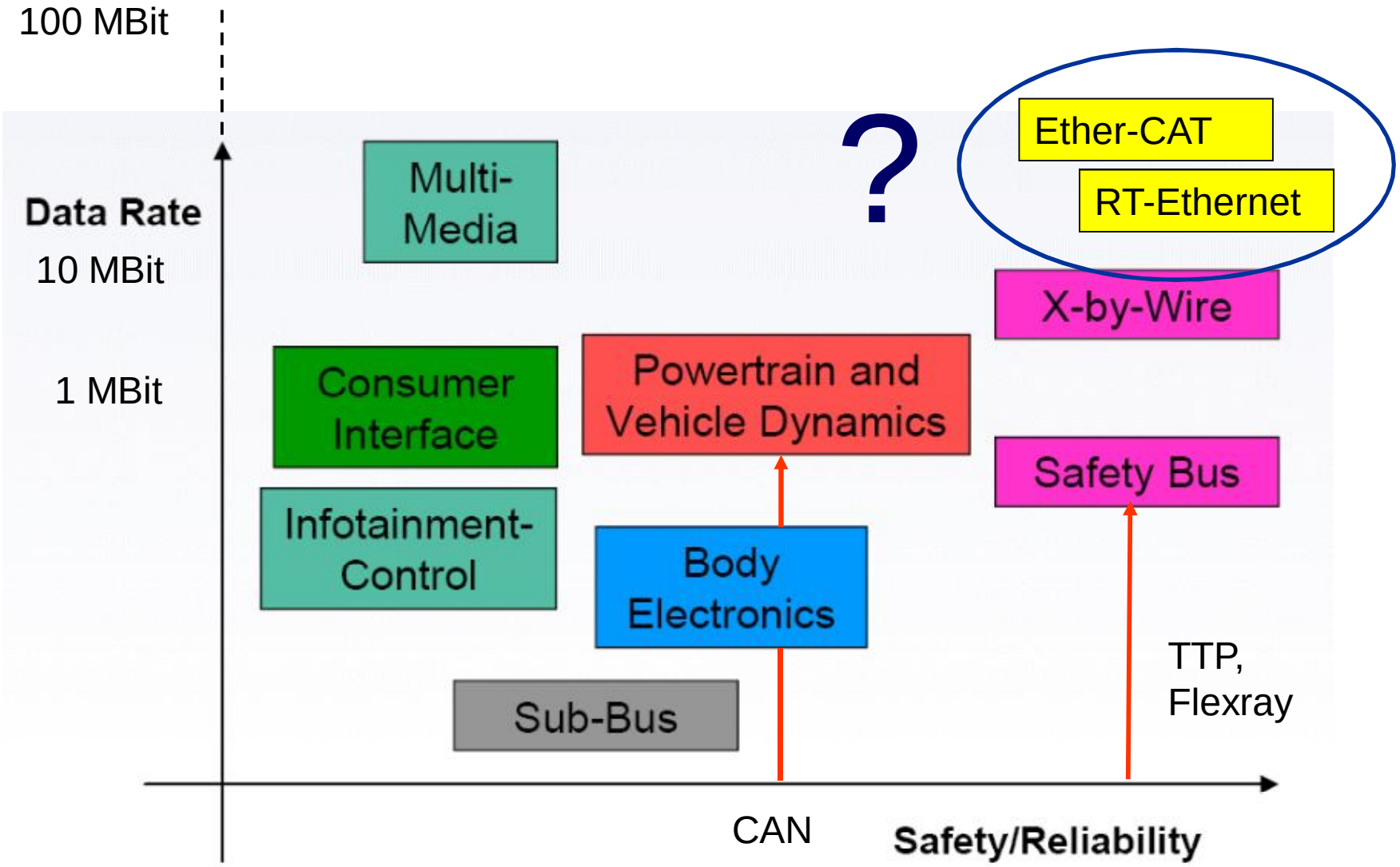
L'unità ricevente dovrà solo eseguire il calcolo a ritroso e verificherà l'effettivo valore all'interno del messaggio: Running Number + Software CRC + Timeout

Ridondanza di canale

La presenza di un solo canale trasmissivo offre solo la possibilità di portare il sistema in condizioni *Fail Silent* alla perdita del canale.
In caso ciò non fosse possibile è necessario prevedere la ridondanza del canale trasmissivo, che è anche la strada offerta da tutti i sistemi di rete più evoluti orientati alla sicurezza.



Quali prospettive nelle reti embedded?



Caratteristiche e performance dei CAN Triggered

Negli ultimi anni le maggiori aziende produttrici di auto hanno progettato e testato una nuova generazione di reti per il mercato automotive: I CAN triggered.

- Comunicazione “Time Triggered” al posto del tradizionale metodo di comunicazione CAN “Event Triggered”
- Network speed: fino a 25 MBit/s
- Massima lunghezza dei frame: fino a 246 byte di dati per messaggio
- Sincronizzazione delle diverse unità in rete: sincronizzazione del clock di rete *fault tolerant*
- Fault tolerance: *single hardware fault tolerance*; possibilità di implementare un singolo canale di rete or un doppio canale ridondante
- Tempo di ritardo della rete Deterministico
- Comunicazione di tipo TDMA/FTDMA, *overhead* di trasmissione ridotto ed elevata efficienza di uso del tempo di rete
- Topologie di rete flessibili e adattabili alle esigenze delle applicazioni: topologie di rete attive con livello di sicurezza funzionale maggiore rispetto alle tradizionali reti CAN