

High Integrity of Communications in Networks for Critical Control Systems

A. Youssef, Y. Crouzet
A. de Bonneval, J. Arlat

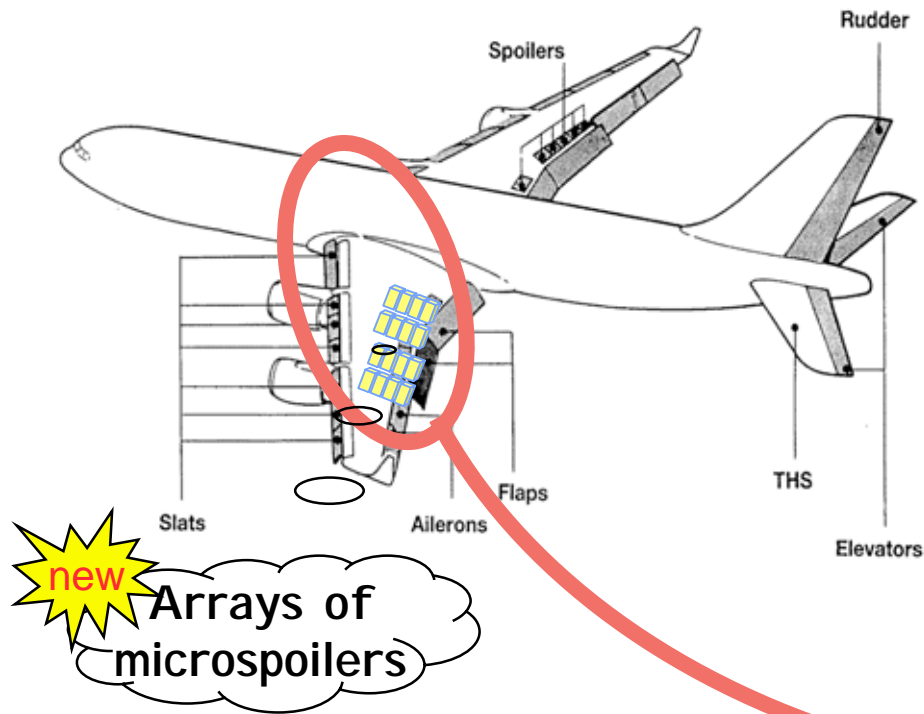


J.-J. Aubert, P. Brot



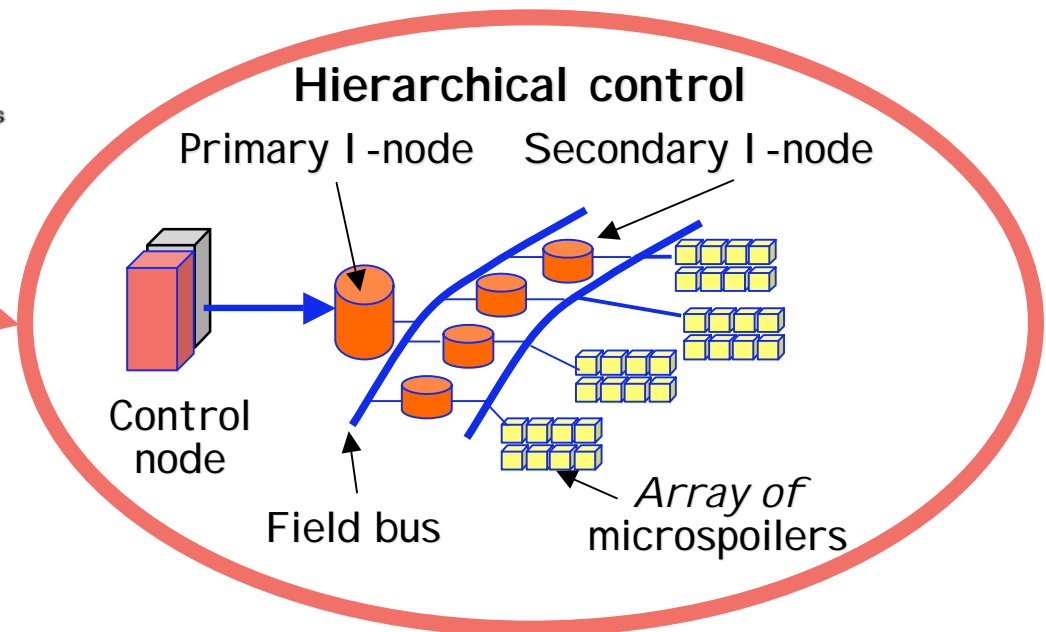
Context and Motivation

- Usage of fully-digital communication networks into critical embedded systems (commercial aircraft architecture)



- Flexible control

- ◆ accommodate distinct commands on different actuators
- ◆ -> all devices cannot be connected to the same bus
- ◆ Need for **intermediate functional nodes** "I-nodes" (not simple repeaters)

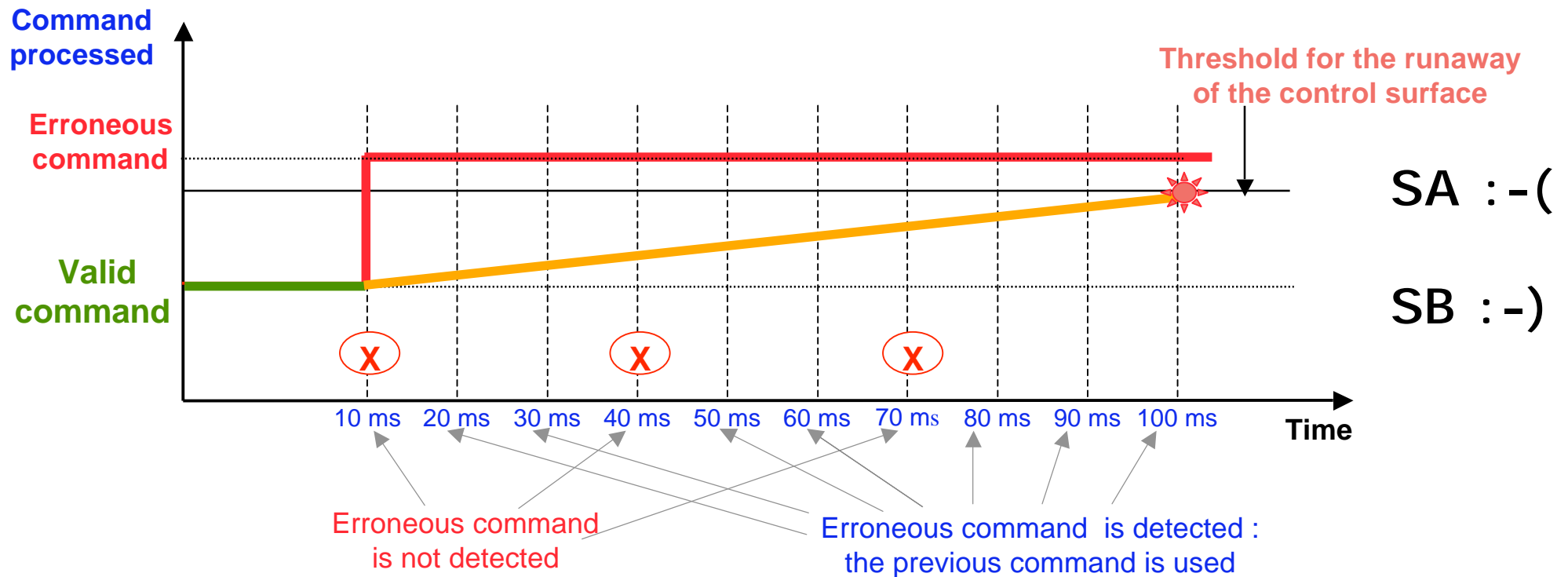


Baseline

- **Slow dynamics of the process** (more than one erroneous command sustained before leading to an undesired event)
 - > **Option to (re-)use previous command (even erroneous)**
- **Undesired Event (UE) = "Runaway" of the controlled surface**
 - > Discrepancy wrt nominal reference value $\geq 5^\circ$
[servomechanisms with max. speed movement of $50^\circ/\text{s}$]
 - Erroneous reference value applied for $\geq 100\text{ms}$ (10 cycles) => UE**
- **Safety requirement "risk of undesired event $\leq 10^{-9}/\text{h}$ "**
 - > **Constraint on communication system integrity**
 - "Number of undetected erroneous messages < threshold t "**
- **Recovery (mitigate issues) -> back-up actions**
 - ◆ Ensure the correct updating of the reference value to the servomechanism
 - ◆ Do not discard too quickly the communication system
 - ◆ Do not impair the required safety level

About Recovery and Undesired Event

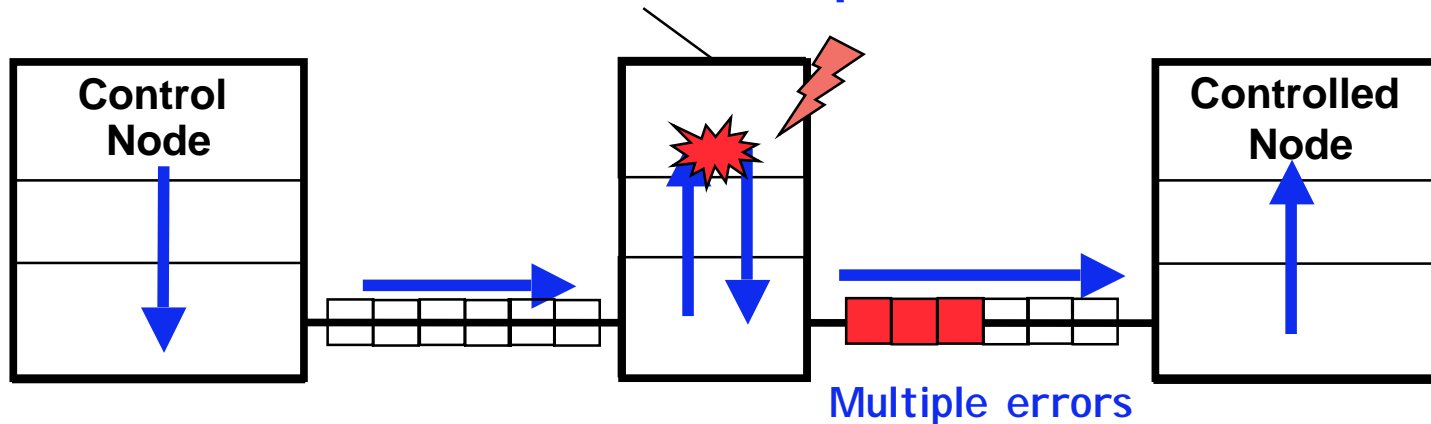
- Re-use of the previous (“correct”) command and “filtering”:
 - ◆ SA) launch the recovery after r consecutive processing cycles for which an error has been signaled;
 - ◆ SB) launch the recovery after r processing cycles for which an error has been signaled out of a window of w successive cycles
- Example ($w = 10$ and $r = 3$)



Target UE = Reception of 3 erroneous message in set of 10 cycles 4

Impact of Intermediate Nodes

Intermediate nodes process data

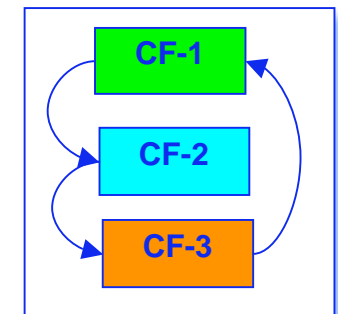


■ Classical approaches: -> Inefficient and/or improper

- ◆ Basic coding techniques (CRCs)
- ◆ End-to-end detection mechanisms (HEDC, Keyed CRC, Safety Layer)

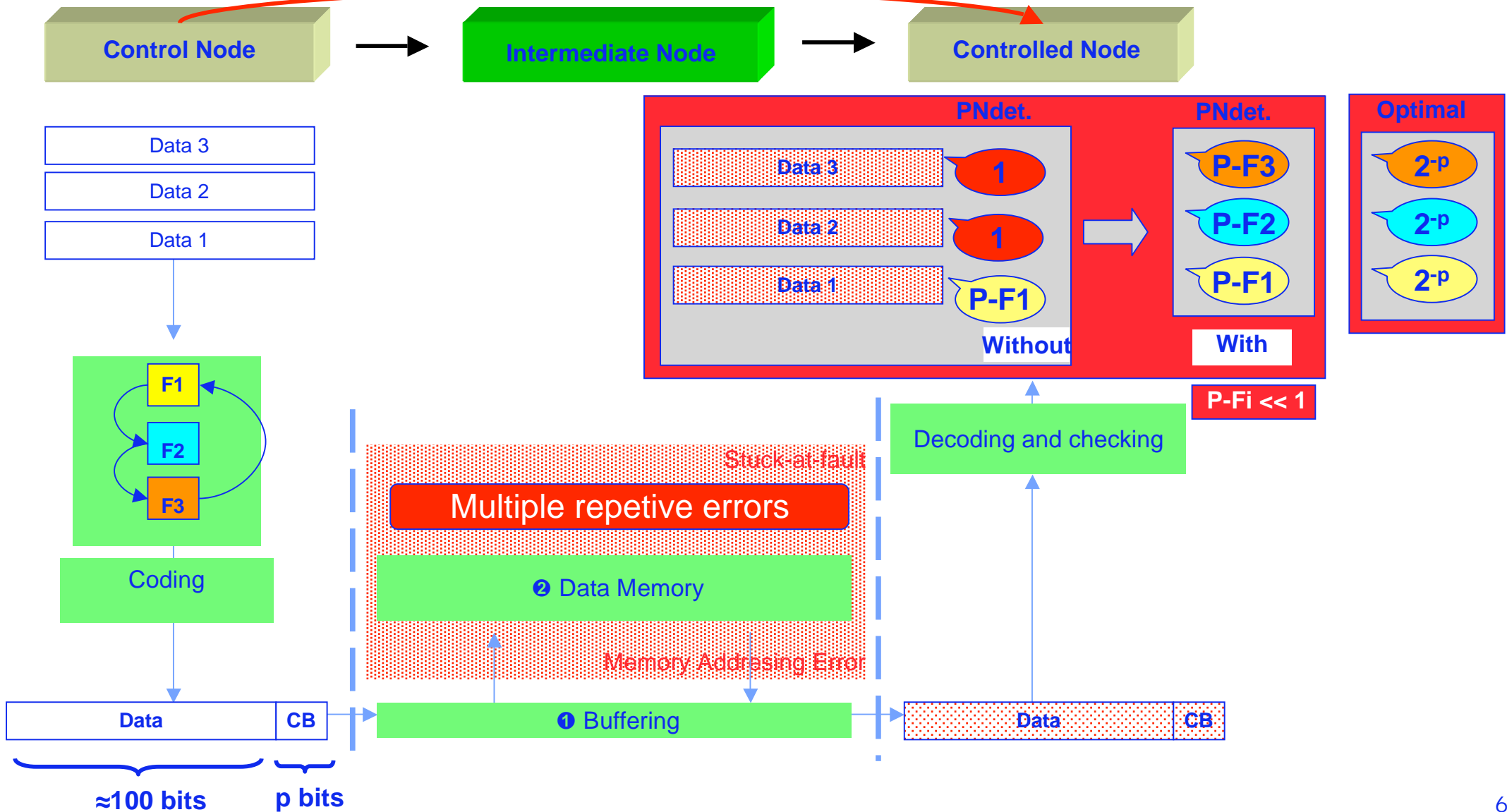
—> Introduce some degree of diversification

- ◆ data and redundancy (e.g., TMR)
- ◆ data and coding (Turbo Codes)
- ◆ coding function (e.g., rotation of the coding function)
Multiple Error Coding Function ->
($m = 3$)

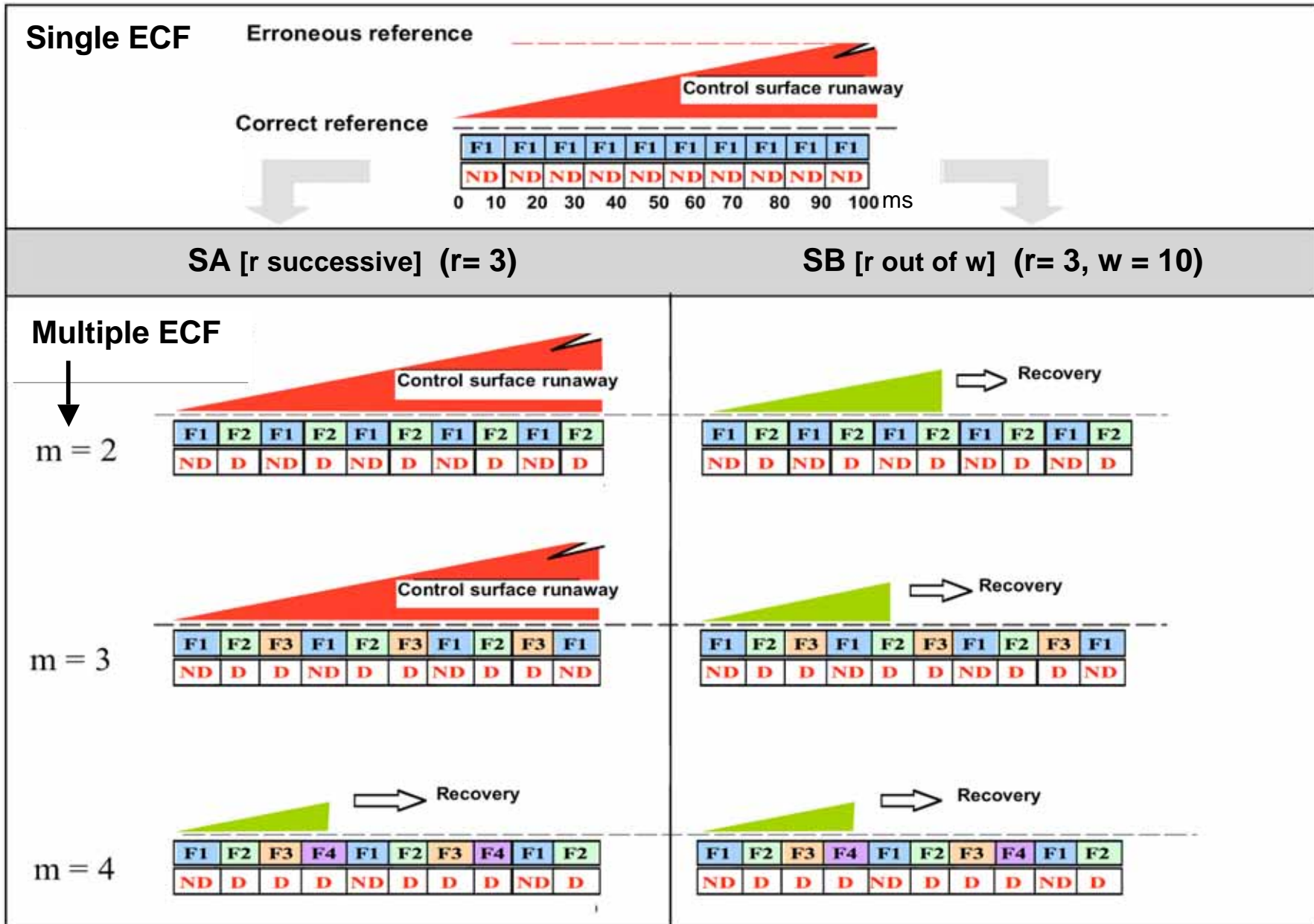


Principle and Benefit

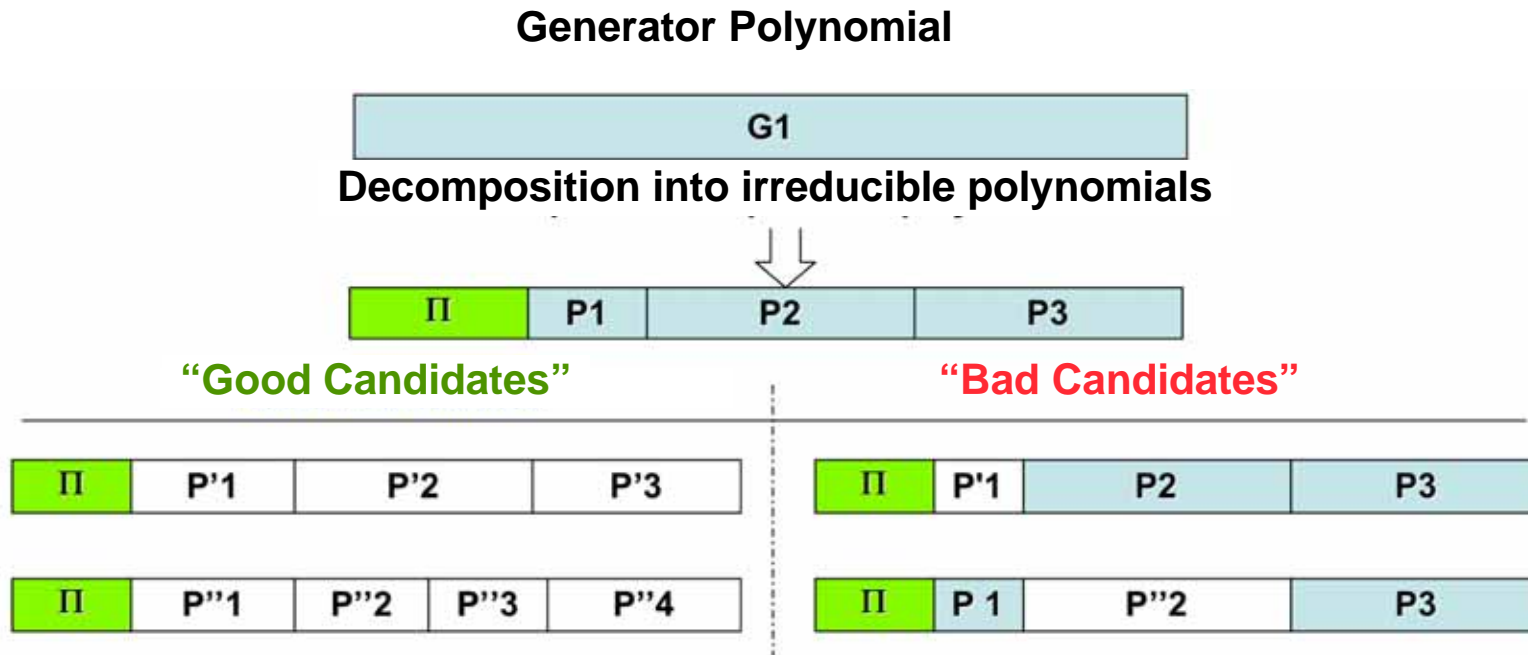
High Integrity Requirement



Impact on Detection and Recovery



Implementation Using CRCs



- Π = small degree polynomial featuring “standard” error detection properties (e.g., $[1+x]$)
- P'_i and $P''_i \neq P_i \forall i$

Generator Polynomial Selection

$$G_1(x) = (1+x) \cdot (1+x+x^7) \cdot (1+x^2+x^3+x^4+x^8) = 1+x^3+x^5+x^6+x^7+x^9+x^{10}+x^{12}+x^{15}+x^{16}$$

Examples of Potentially Good Candidates

$$G_*(x) = (1+x) \cdot 7\text{-degree irreducible polynomial} \cdot 8\text{-degree irreducible polynomial}$$

Identifier	Polynomial representation	Decomposition into irreducible polynomials
$G_2(x)$	$1+x+x^6+x^7+x^8+x^9+x^{10}+x^{13}+x^{15}+x^{16}$	$(1+x) \cdot (1+x+x^3+x^5+x^7) \cdot (1+x+x^2+x^4+x^5+x^6+x^8)$
$G_3(x)$	$1+x+x^6+x^{10}+x^{12}+x^{16}$	$(1+x) \cdot (1+x+x^2+x^3+x^7) \cdot (1+x+x^4+x^5+x^6+x^7+x^8)$
$G_4(x)$	$1+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{16}$	$(1+x) \cdot (1+x^3+x^7) \cdot (1+x+x^2+x^5+x^6+x^7+x^8)$

Examples of Potentially Bad Candidates

$$G_*(x) = (1+x) \cdot (1+x+x^7) \cdot 8\text{-degree irreducible polynomial}$$

$G_5(x)$	$1+x+x^2+x^3+x^5+x^6+x^9+x^{10}+x^{12}+x^{14}+x^{15}+x^{16}$	$(1+x) \cdot (1+x+x^7) \cdot (1+x+x^5+x^6+x^8)$
$G_6(x)$	$1+x^3+x^6+x^7+x^{10}+x^{13}+x^{14}+x^{16}$	$(1+x) \cdot (1+x+x^7) \cdot (1+x^2+x^3+x^4+x^5+x^7+x^8)$

This was analyzed and confirmed via extensive simulation runs

Example of Analysis: Target Codes

$$G_a(x) = \underline{(1+x)} \cdot (1+x+x^{15}) = 1+x^2+x^{15}+x^{16} \text{ — Standard generator polynomial : CRC-16}$$

Standard generator polynomials

$$G_*(x) = (1+x) \cdot 15\text{-degree polynomial}$$

Identifier	Polynomial representation	Decomposition into irreducible polynomials
$G_b(x)$: IEEE-WG 77.1	$1+x+x^5+x^6+x^8+x^9+x^{10}+x^{11}+x^{13}+x^{14}+x^{16}$	$(1+x^2+x^3+x^4+x^8) \cdot (1+x+x^2+x^4+x^5+x^6+x^8)$
$G_c(x)$: CRC-CCIT T	$1+x^5+x^{12}+x^{16}$	$\underline{(1+x)} \cdot (1+x+x^2+x^3+x^4+x^{12}+x^{13}+x^{14}+x^{15})$
$G_d(x)$: IBM-SDLC	$1+x+x^2+x^4+x^7+x^{13}+x^{15}+x^{16}$	$\underline{(1+x)}^2 \cdot (1+x+x^3+x^4+x^5+x^6+x^8+x^{10}+x^{12}+x^{13}+x^{14})$
$G_e(x)$: CRC-16Q*	$1+x+x^3+x^4+x^5+x^6+x^8+x^{11}+x^{15}+x^{16}$	$\underline{(1+x)} \cdot (1+x^3+x^5+x^8+x^9+x^{10}+x^{15})$
$G_f(x)$: IEC-TC 57	$1+x+x^4+x^7+x^8+x^9+x^{11}+x^{12}+x^{14}+x^{16}$	$\underline{(1+x)}^2 \cdot (1+x+x^3+x^6+x^7) \cdot (1+x^2+x^3+x^4+x^5+x^6+x^7)$

Custom generator polynomials

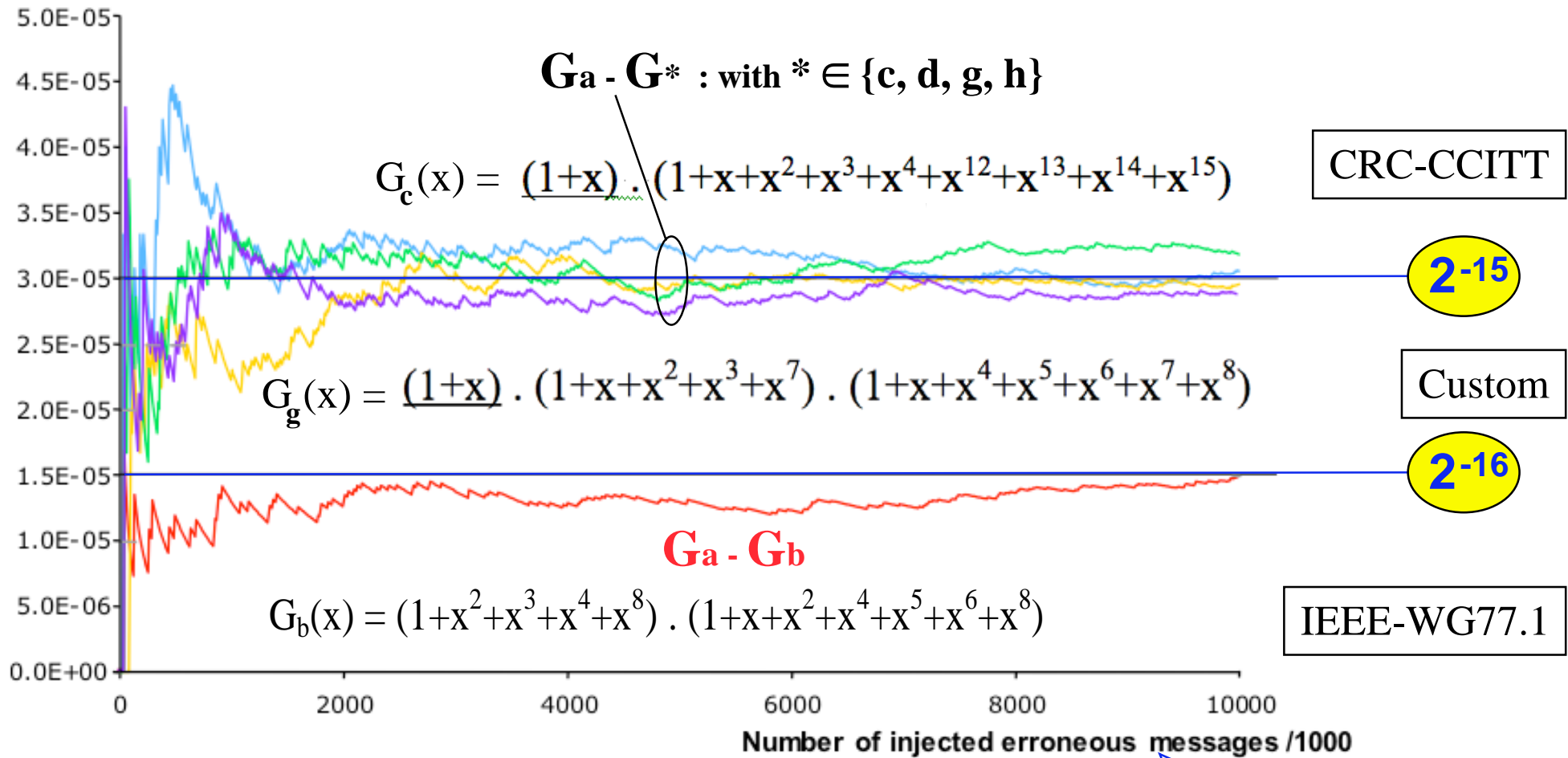
$$G_*(x) = (1+x) \cdot 7\text{-degree irreducible polynomial} \cdot 8\text{-degree irreducible polynomial}$$

$G_g(x) = G_3(x)$	$1+x+x^6+x^{10}+x^{12}+x^{16}$	$\underline{(1+x)} \cdot (1+x+x^2+x^3+x^7) \cdot (1+x+x^4+x^5+x^6+x^7+x^8)$
$G_h(x) = G_4(x)$	$1+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{16}$	$\underline{(1+x)} \cdot (1+x^3+x^7) \cdot (1+x+x^2+x^5+x^6+x^7+x^8)$

Examples of Simulation Runs

$$G_a(x) = (1+x) \cdot (1+x+x^{15}) \cdot (1+x^3+x^{15}+x^{16})$$

CRC-16



CRC-CCITT

2-15

Custom

2-16

IEEE-WG77.1

Concluding Remarks

- Pragmatic Approach for Mitigating High Integrity Requirements in Critical Communications Systems
- CRC-based Implementation:
 - ◆ Theoretical issues associated to properties of generator polynomials provide a sound basis for identifying criteria for selecting suitable coding functions
 - ◆ Criteria validated via extensive simulation runs
- Generalization: investigation of alternative policies for mixing distinct coding functions (CF)
- Formalization: derivation of closed-form expressions
 - ◆ Probability of undetected errors (PUE)
 - ◆ (Min) Latency for system recovery action after an error is undetected (LRA)
[# of message cycles]

Example: $m > 1$ # of distinct CF; r # of reported error detections,
 w size of window (for SB, only)

LRA(SA) = $r+1$ for $r < m$; LRA(SB) = $\lceil m \times r / (m - 1) \rceil$ for $LRA < w$