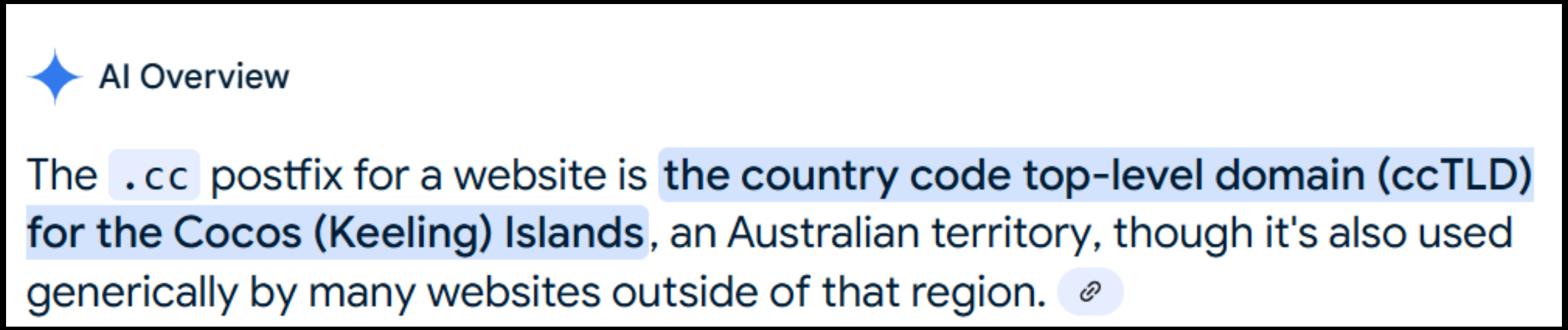
How Automotive Functional Safety Is Disrupting Design Methodologies

Charles (Chuck) Alpert, Ph.D.
Fellow
Silicon Verification Group, Cadence

Agentic AI Focus

- Still doing automotive
- Hiring folks with both AI and EDA expertise
- Opportunities for academia / industry collaboration (Netcast TAB)
- Maybe I can give another talk at ISPD 2026??

Why www.ispd.cc?



cc == cool conference

Major Growth Opportunity Unleashed by Automotive Innovation

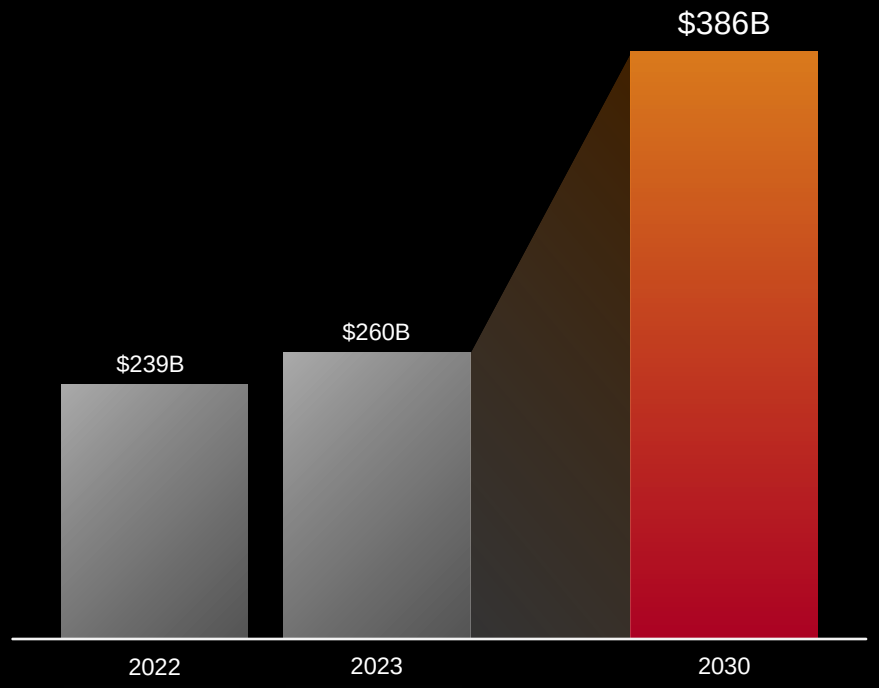
14%
OF NEW CARS EVS

70+
SENSORS IN CAR

- Connectivity
- Vehicle Management
- Predictive Maintenance

STATISTA, 2023

AUTOMOTIVE ELECTRONICS MARKET



SOURCE FORTUNE BUSINESS INSIGHTS, "2023 AUTOMOTIVE ELECTRONICS MARKET"

60%
OF NEW CARS EVS

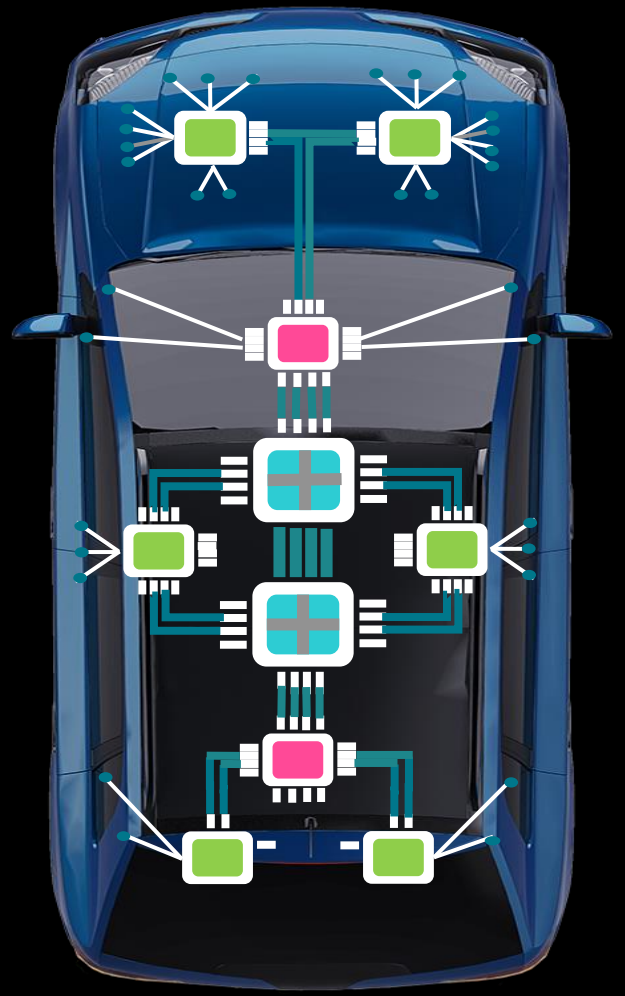
200+
SENSORS IN CAR

- Autonomous Driving
- Next-Generation Infotainment
- Smart Vehicle Integration

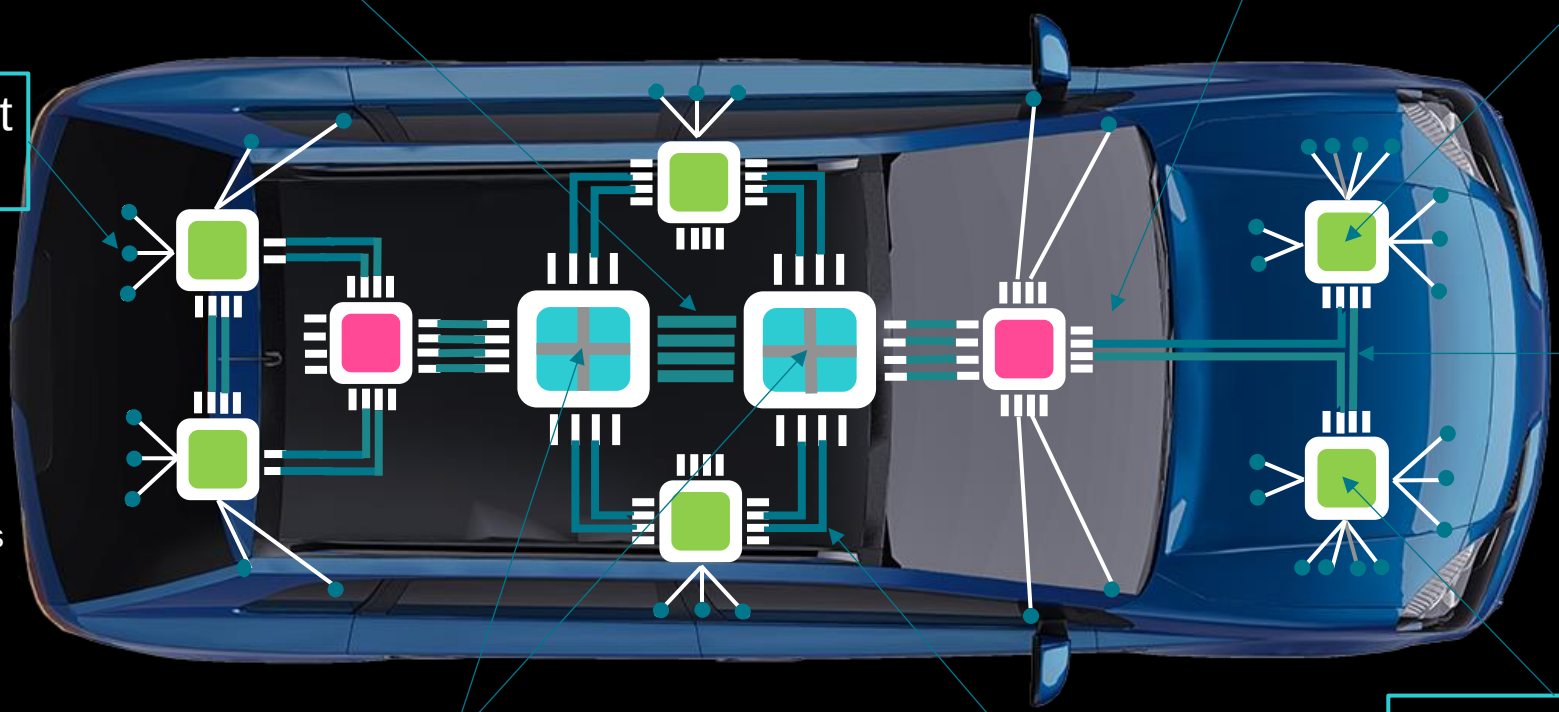
IEA, 2022

Automotive Market Trends

Data Center on Wheels
Software-Defined Vehicle



The Trend Toward Zonal Architecture



High-Speed Ethernet Backbone

Intelligent Gateway

Multi-Functional Zone Controllers

High-Speed Endpoint Connections

Scalable Architecture

MIPI®, PCIe®,...

Ethernet

Zonal Endpoints

Gateway ECU

Zonal ECU

Central ECU

Redundant Central CPUs

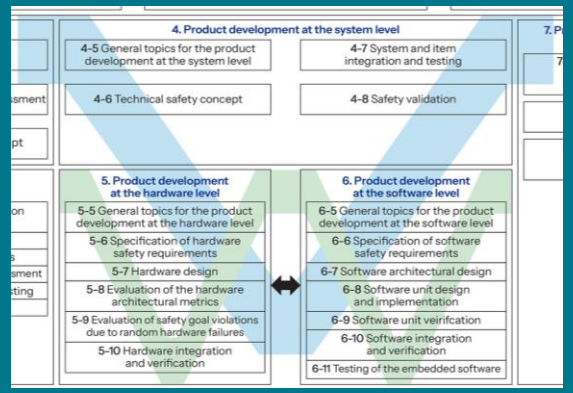
Network Consolidation

ECU Consolidation

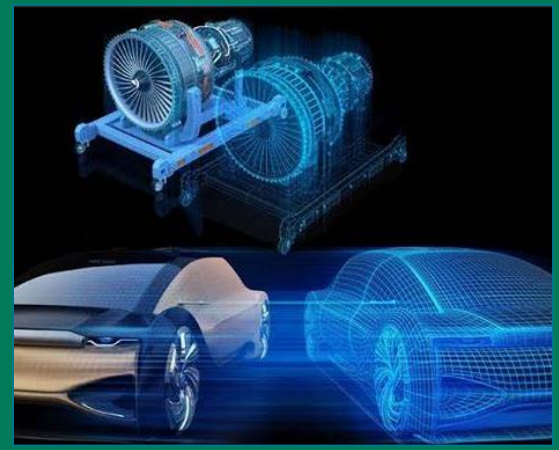
Cadence Automotive Offerings

Chiplets and IP

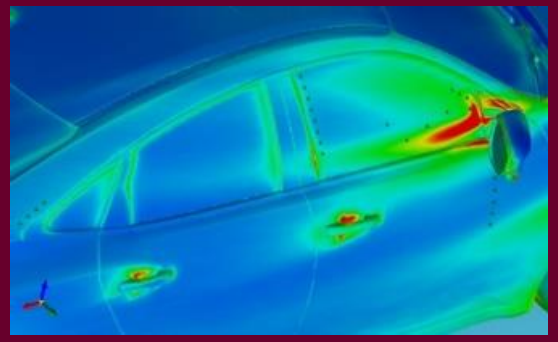
Functional Safety



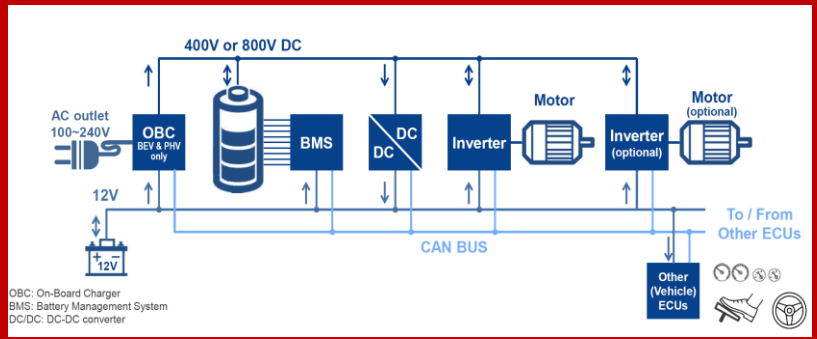
Digital Twins



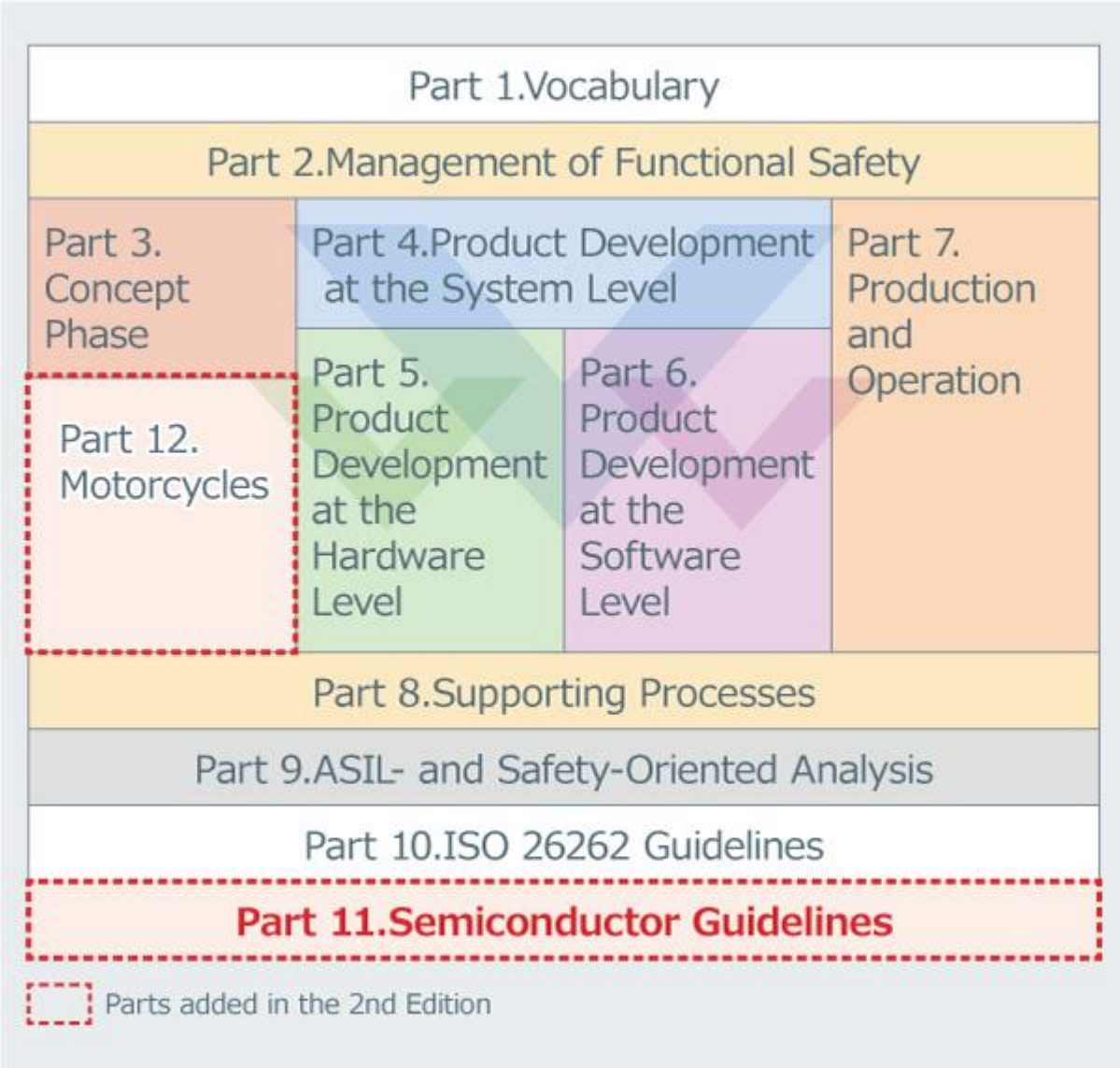
Multiphysics



Power Management



ISO 26262: Road Vehicles – Functional Safety (FuSa)



Functional safety: The ability of a system to respond correctly to both expected and unexpected inputs to reduce the risk of accidents

ISO 26262: 700+ pages in 12 sections

FuSa adherence increases: Time, cost, testing, validation, documentation

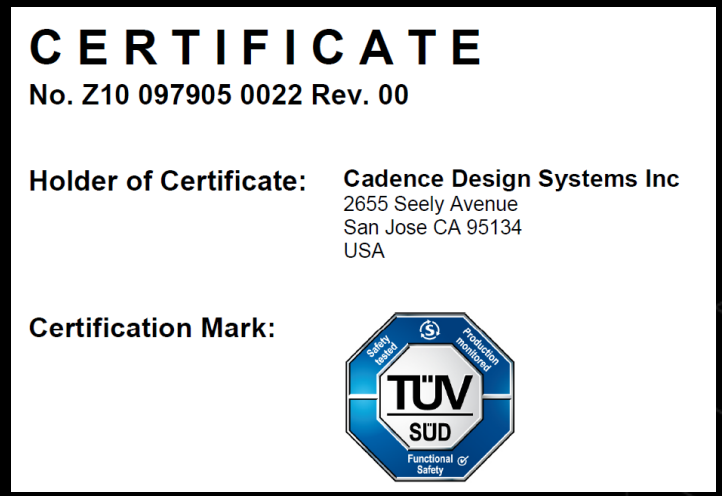
How to Meet ASIL Standards

FIT (Failures in time): Number of failures per billion hours

SPFM (Single point fault metric): Fault ratio to measure design robustness

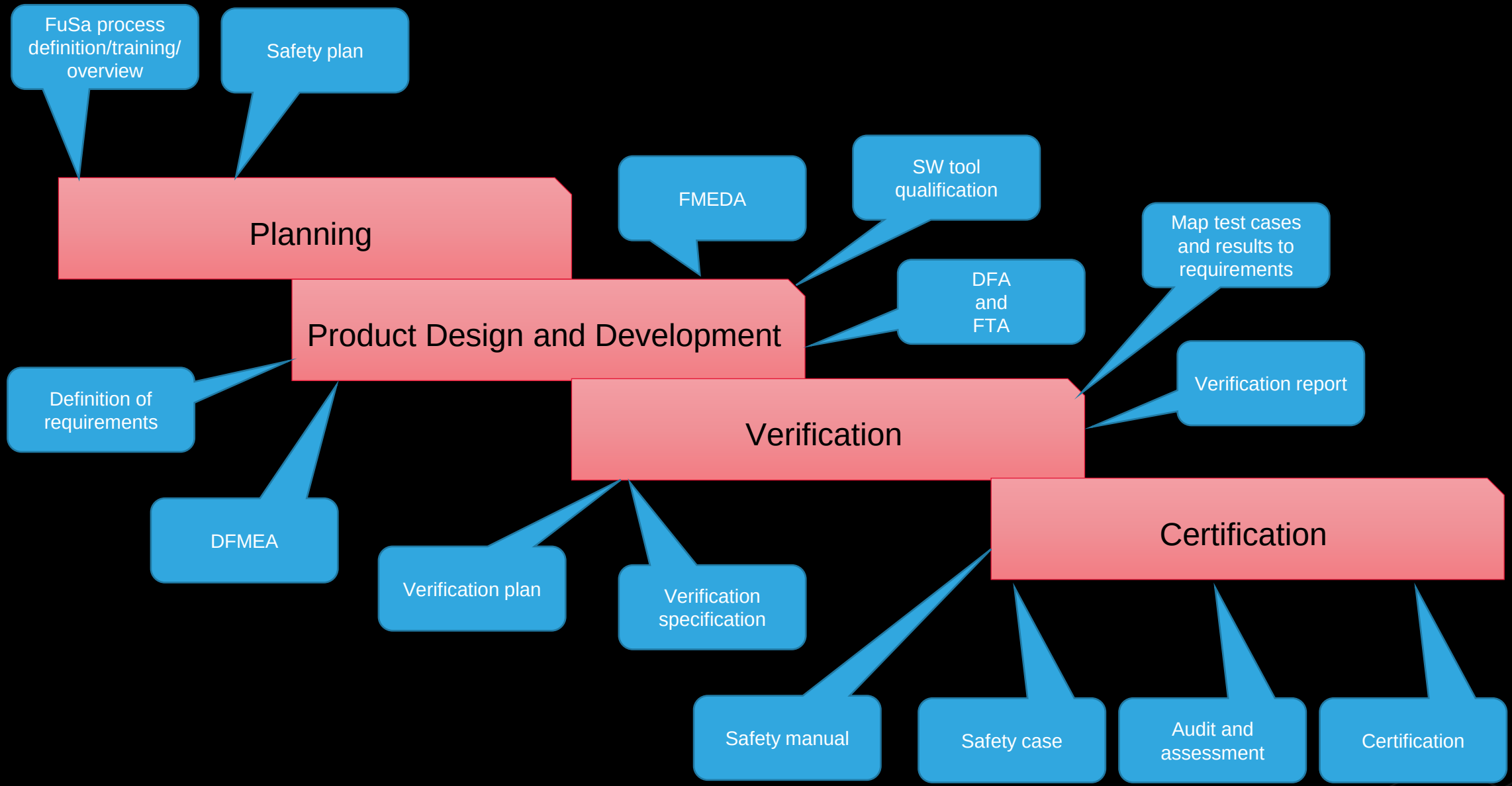
LFM (Latent fault metric): Same as SPFM but for multiple faults

ASIL	FIT	SPFM	LFM
QM	N/A	N/A	N/A
A	N/A	N/A	N/A
B	< 100	> 90%	> 60%
C	< 100	> 97%	> 80%
D	< 10	> 99%	> 90%



cadence

ASIL-Compliant FuSa Activities in HW Product Development Flow

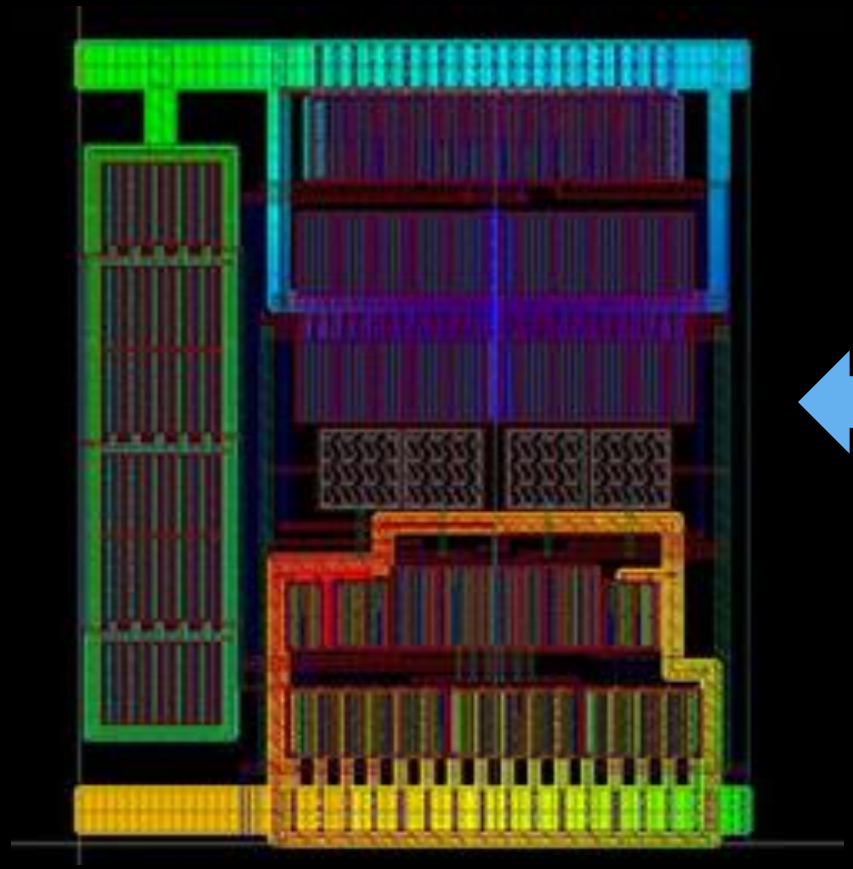


Hardware Safety Mechanism Overview

Watchdog Timers

Redundant Logic

Safe Shutdown Circuits



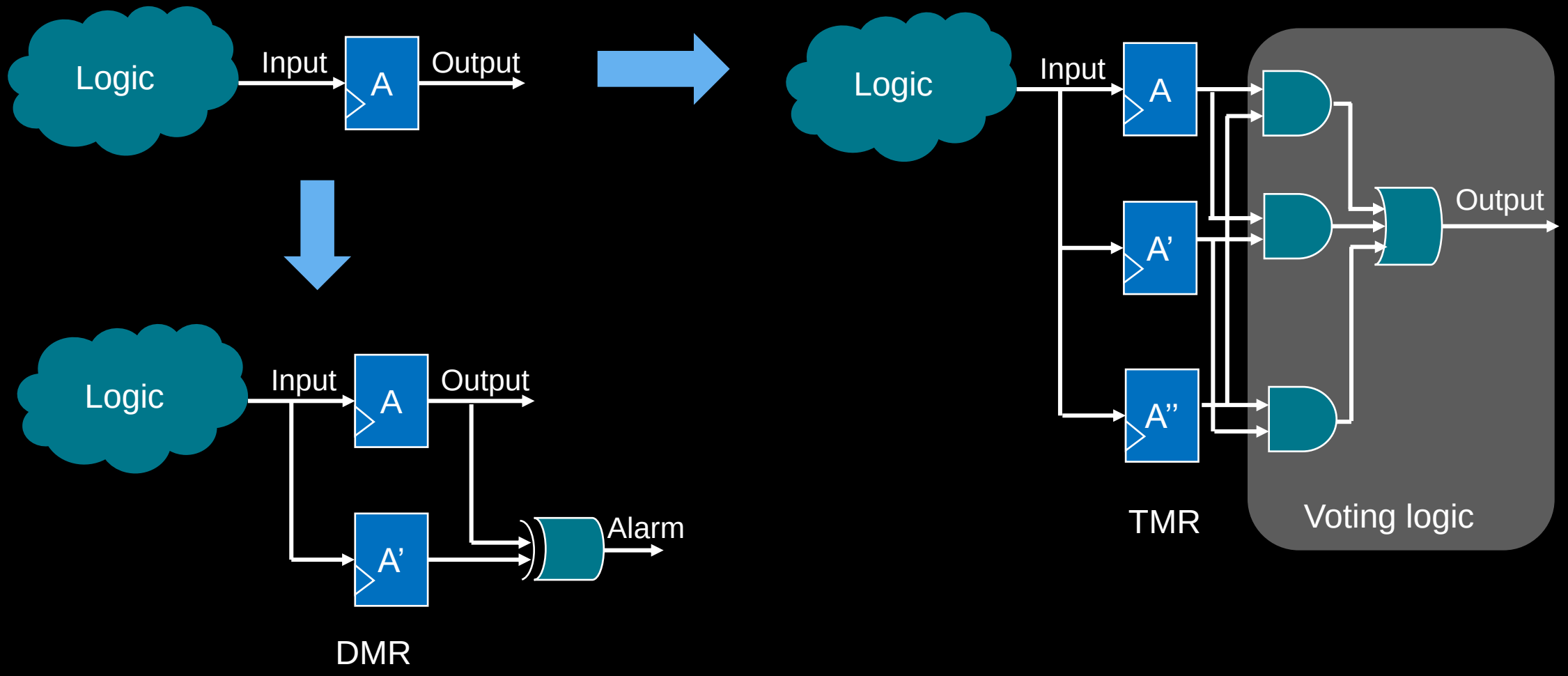
Error Correcting Codes

Soft Error Resilient Flops

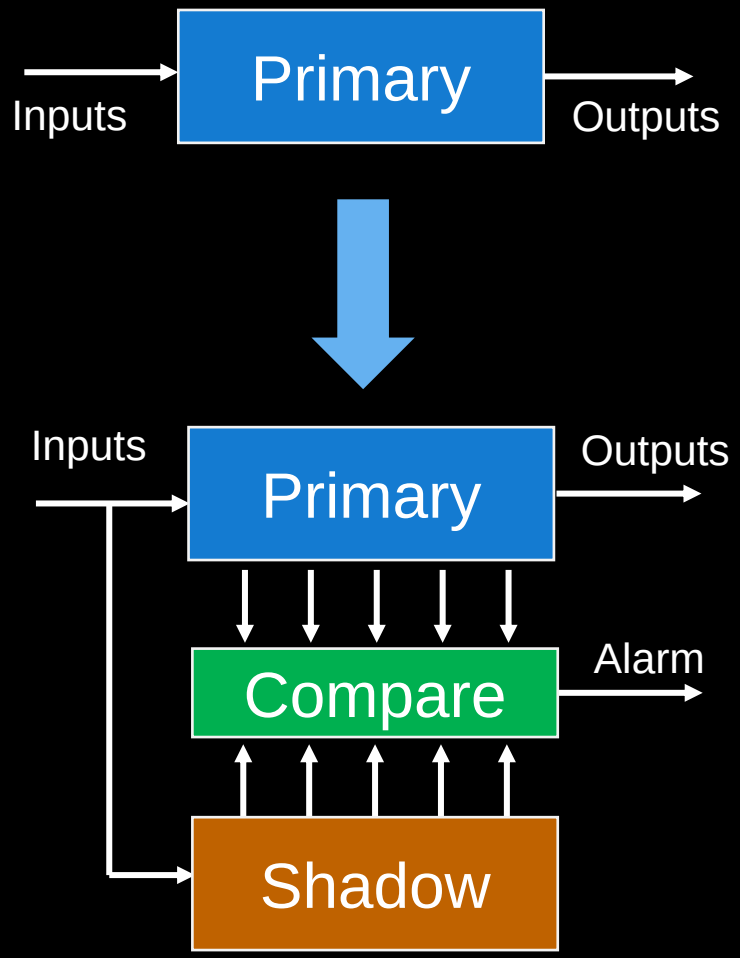
LBIST and MBIST

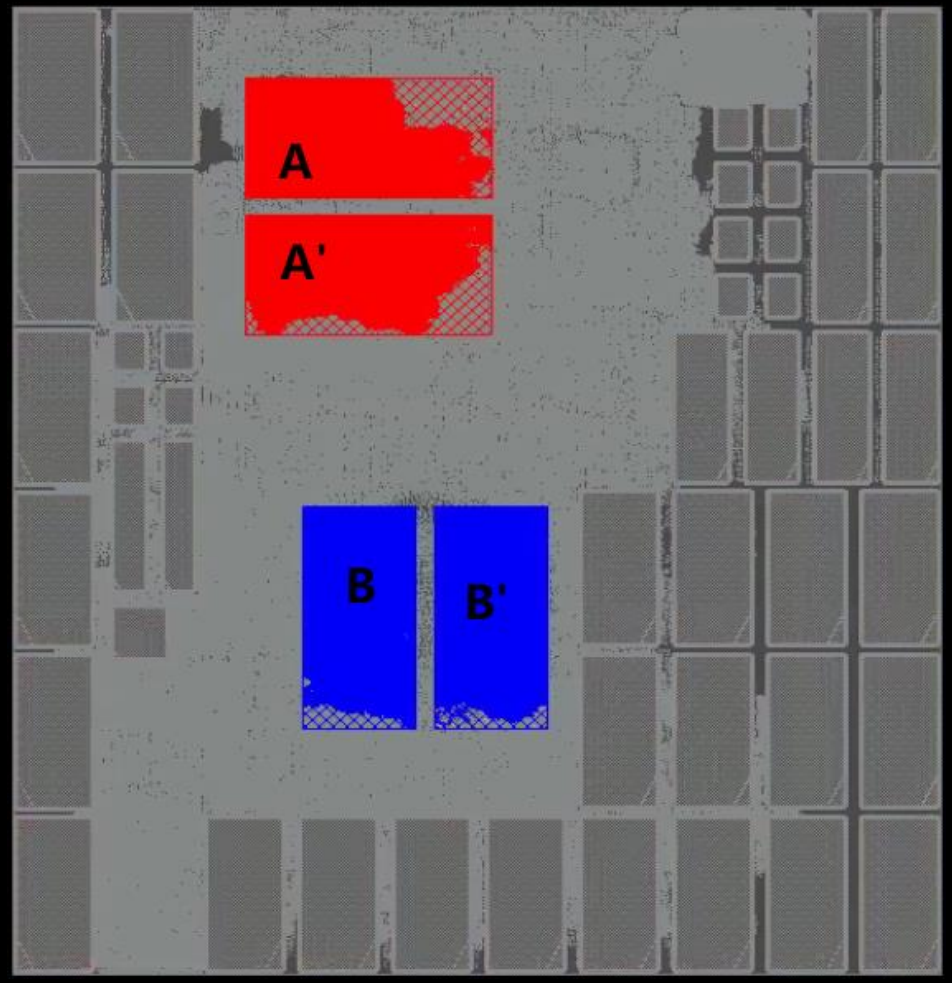
Significant area overhead for safety mechanisms
Perhaps 40% for ASIL-B, 80% for ASIL-D

Dual and Triple Modular Redundancy

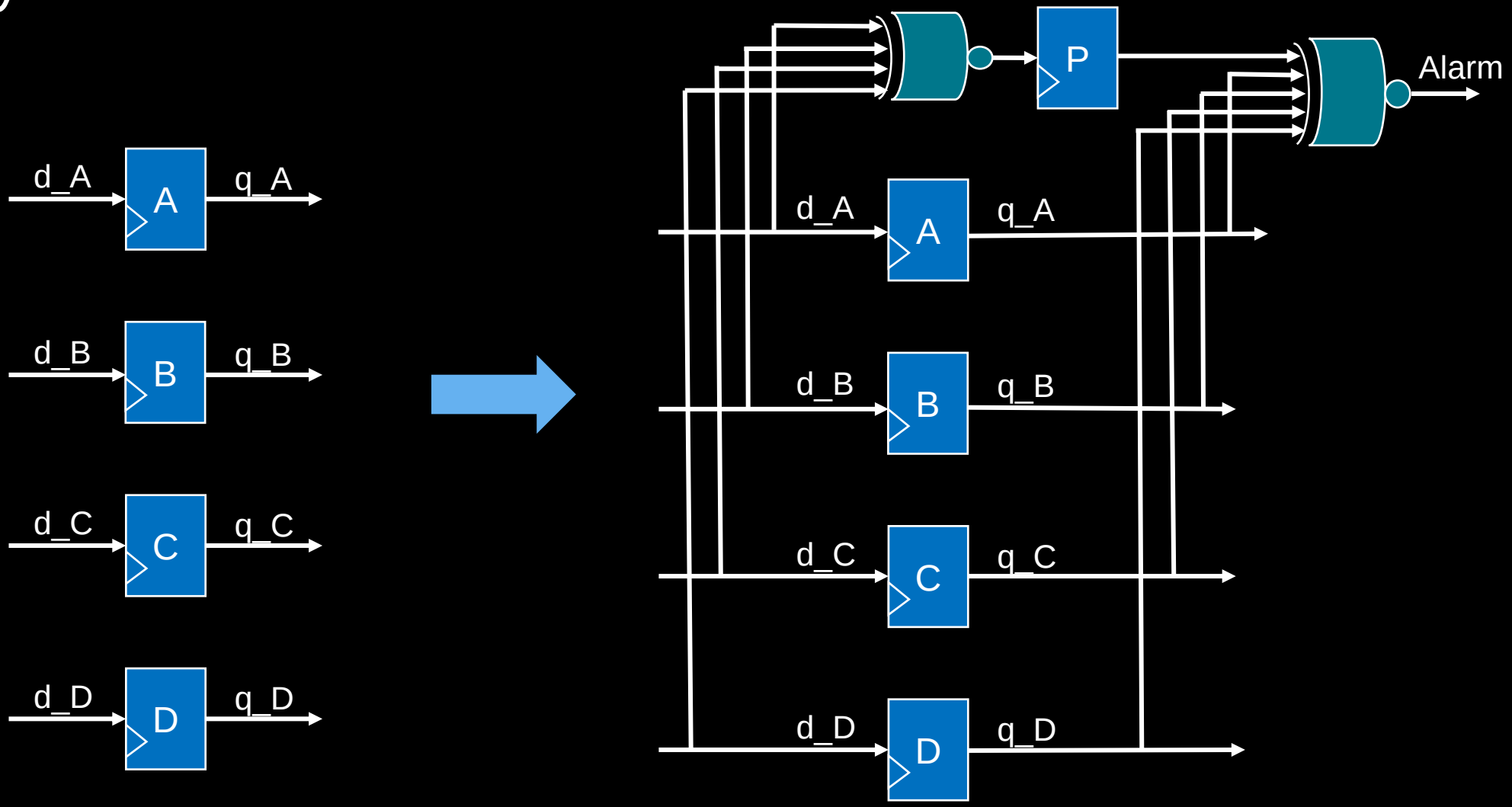


Hardware Redundancy (Dual-Core Lock Step or DCLS)





Parity



A Magic Trick

1	3	5	7	9	11	13	15
17	19	21	23	25	27	29	31
33	35	37	39	41	43	45	47
49	51	53	55	57	59	61	63

8	9	10	11	12	13	14	15
24	25	26	27	28	29	30	31
40	41	42	43	44	45	46	47
56	57	58	59	60	61	62	63

2	3	6	7	10	11	14	15
18	19	22	23	26	27	30	31
34	35	38	39	42	43	46	47
50	51	54	55	58	59	62	63

16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

4	5	6	7	12	13	14	15
20	21	22	23	28	29	30	31
36	37	38	39	44	45	46	47
52	53	54	55	60	61	62	63

32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

1 + 8 + 32 = 41

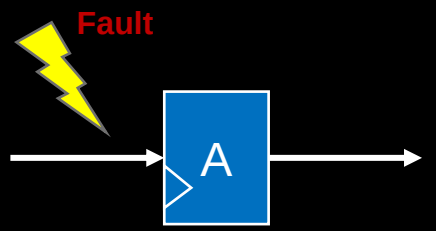
Each card is a parity bit

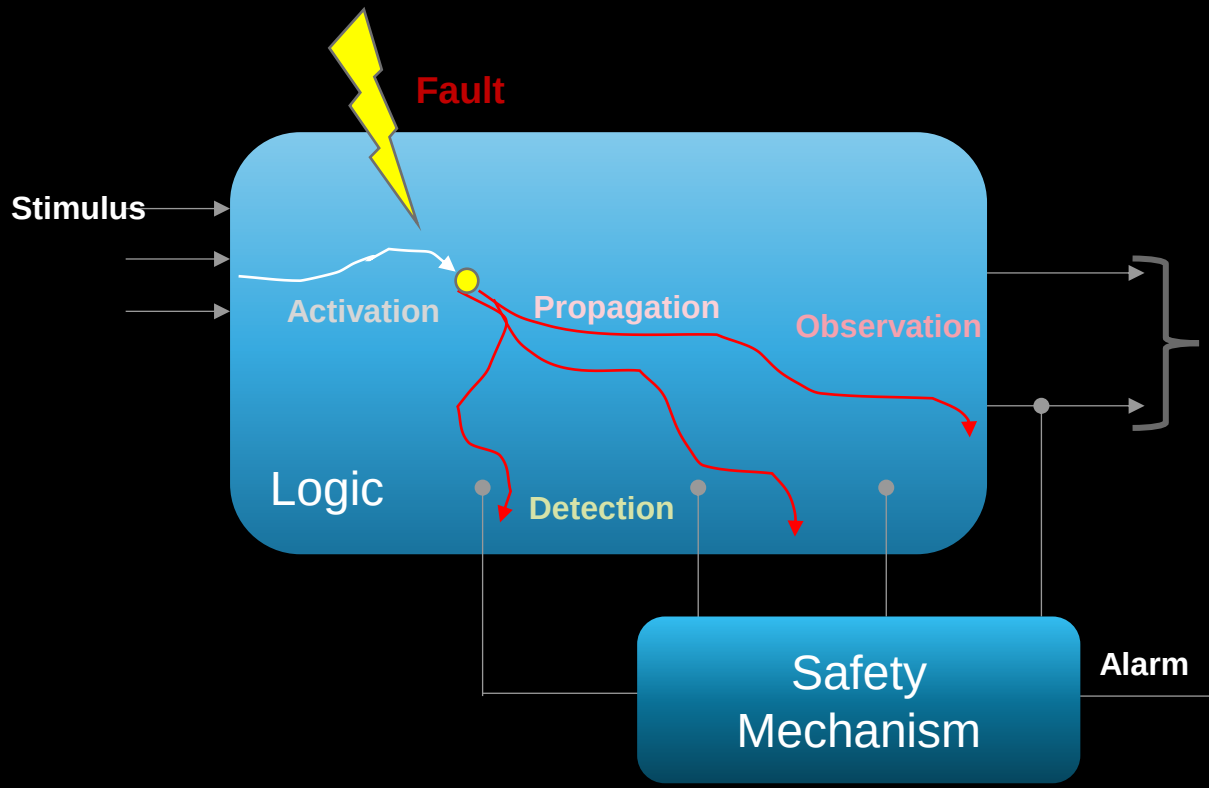
Additional bits for decoding and data correction

Measuring a Safety Mechanism Through Fault Injection

Main idea:
- Force incorrect behavior
- Simulate
- Compare to “good machine”

Three types of faults:
- Stuck at 1
- Stuck at 0
- Single-event upset





Possible Scenarios
- Fault is safe
- Fault propagated to FO and CO
- Fault propagate to FO but not CO
- Fault undetected

Example FMEDA (Failure Mode, Effects, and Diagnostic Analysis)

					SPFM	99.9%
Parts	Sub-Parts	Failure Mode	Safety Goal	λperm [FIT]	Safety Mechanisms	DC
CPU	AHB	Wrong transaction caused by a fault in the AHB interface	SG1	1.01E-02	SM1: DCLS	99.9%
CPU	Decoder	Incorrect instruction flow caused by a fault in the decode logic	SG1	3.92E-03	SM1: DCLS	99.9%
CPU	VIC	Unintended or missing interrupt request	SG1	1.70E-03	SM1: DCLS	99.9%
CPU	Register_ bank_shadow	Wrong data caused by a fault in the register bank shadow	SG1	1.80E-02	SM1: DCLS	99.9%
CPU	Multiplier	Incorrect instruction execution caused by a fault in the multiplier	SG1	9.09E-03	SM1: DCLS	99.9%
CPU	Adder	Incorrect instruction execution caused by a fault in the adder	SG1	2.25E-03	SM1: DCLS	99.9%
CPU	Divider	Incorrect instruction execution caused by a fault in the divider	SG1	1.60E-03	SM1: DCLS	99.9%
CPU	Register_bank	Wrong data caused by a fault caused by a fault in the register bank	SG1	2.96E-02	SM1: DCLS	99.9%
CPU	Pipeline_ctrl	Incorrect instruction timing (too late) due to a fault in the pipeline control	SG1	2.93-E02	SM1: DCLS	99.9%
CPU	Branch_unit	Incorrect instruction flow caused by a fault in the branch logic (Wrong branch prediction affect timing)	SG1	1.04E-03	SM1: DCLS	99.9%
CPU	Fetch	Incorrect instruction flow caused by a fault in the fetch logic	SG1	1.83E-02	SM1: DCLS	99.9%
CPU	Cache	Wrong data cell caused by a cache fault	SG1	3.98E-01	SM1: DCLS	99.9%

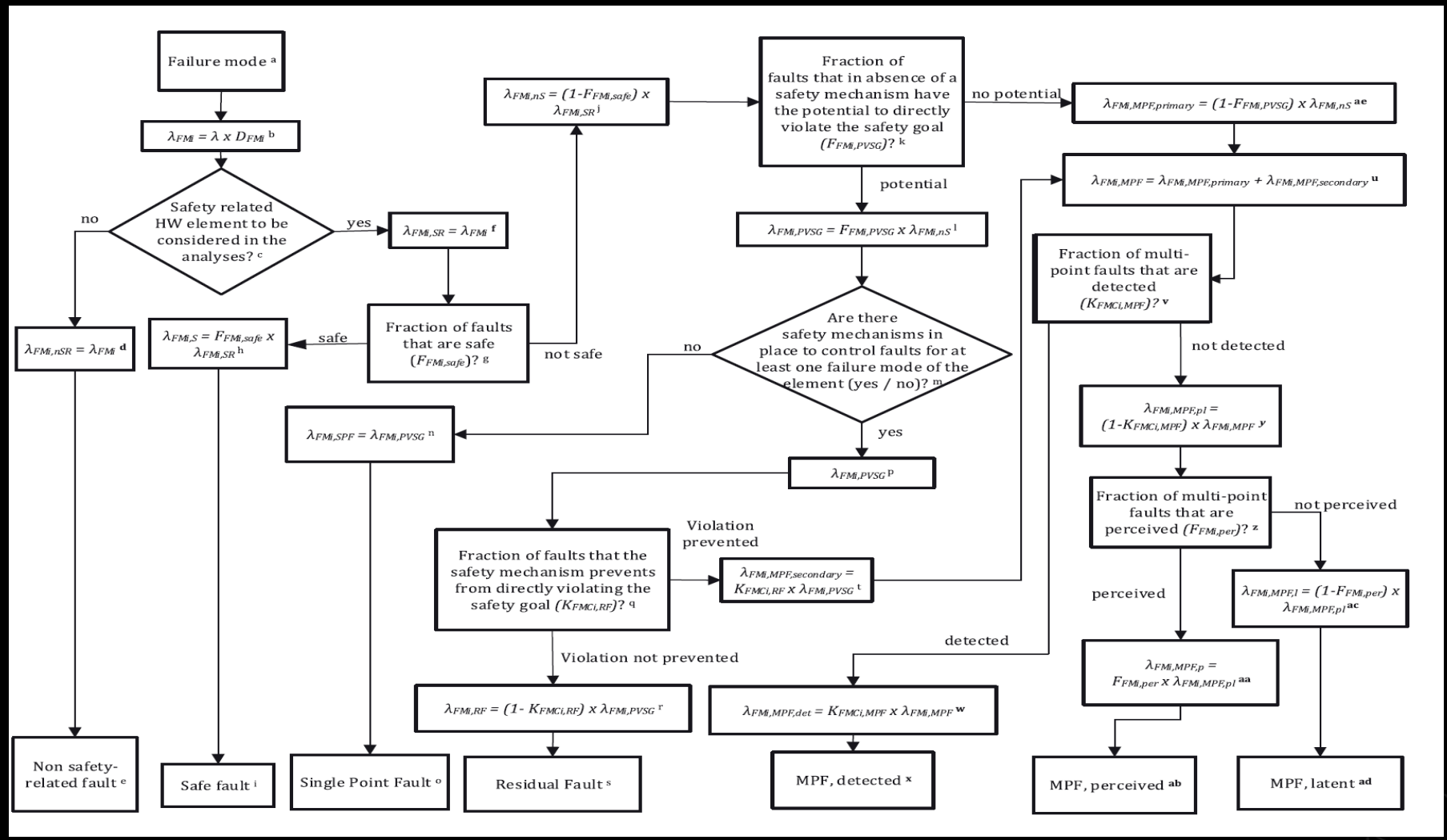
Table 2: Simplified FMEDA table example referred to safety goal SG1 covered by dual-core-lockstep (DCLS)

Calculating ASIL Metrics

Base FIT

$$\lambda = \underbrace{\left\{\lambda_1 \times N \times e^{-0.35 \times a} + \lambda_2\right\} \times \left\{\frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on} + \tau_{off}}\right\}}_{\lambda_{die}} + \underbrace{\left\{2.75 \times 10^{-3} \times \pi_\alpha \times \left(\sum_{i=1}^{z} (\pi_n)_i \times (\Delta T_i)^{0.68}\right) \times \lambda_3\right\}}_{\lambda_{package}} + \underbrace{\left\{\pi_I \times \lambda_{EOS}\right\}}_{\lambda_{overstress}} \times 10^{-9} / h$$

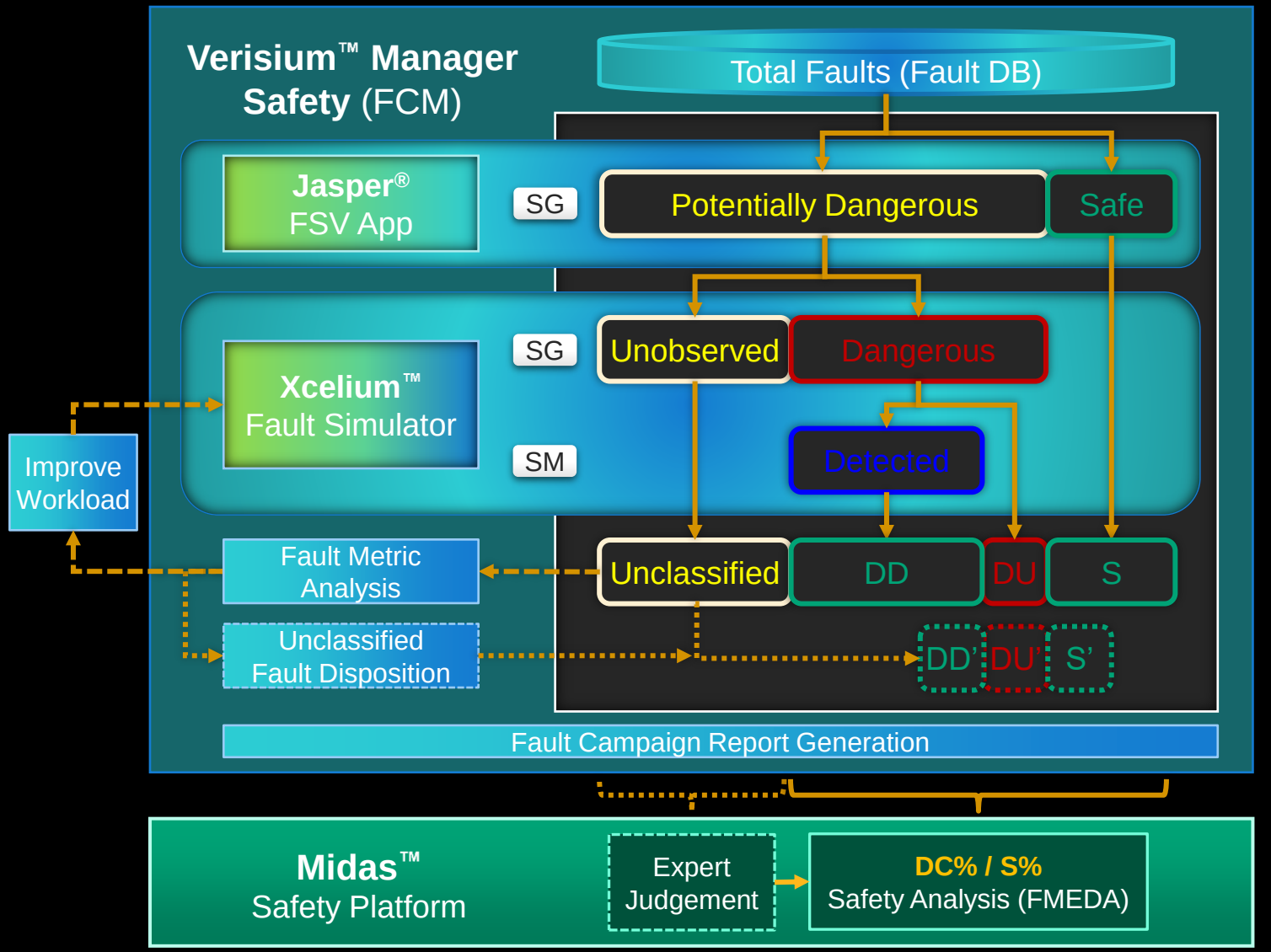
Fault Classification



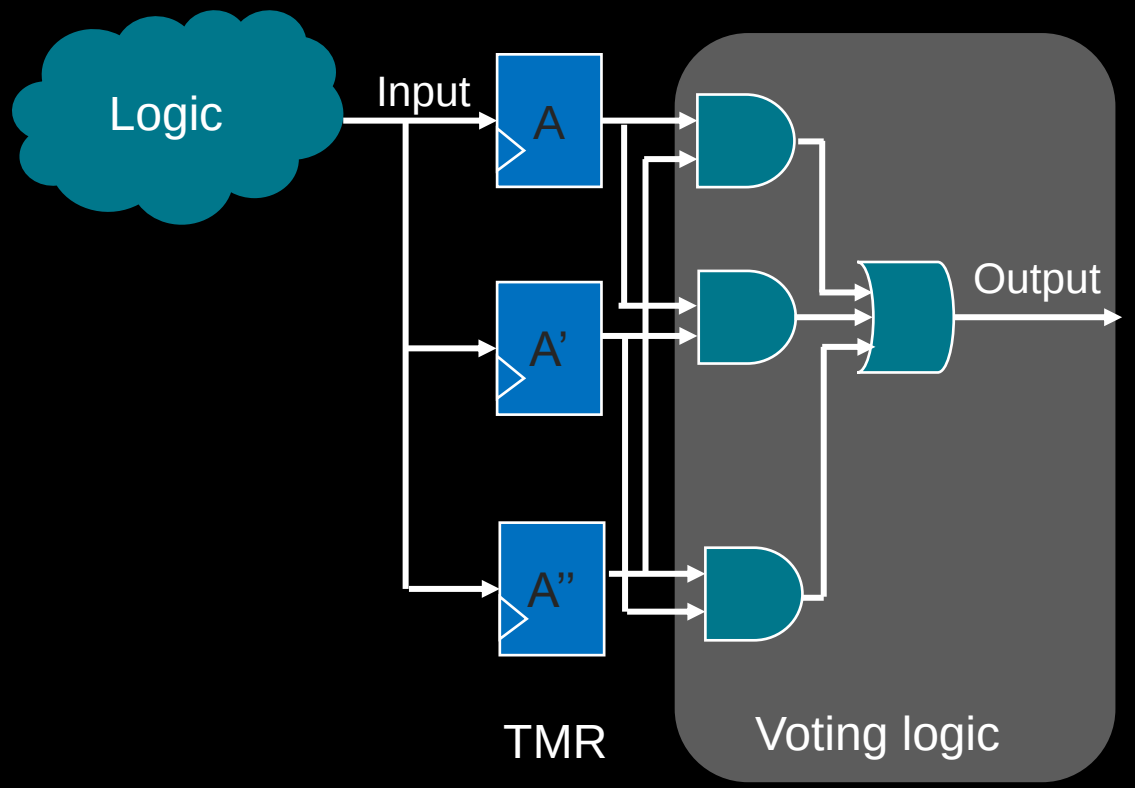
Cadence Functional Safety Solution

Digital Implementation Safety Mechanism Insertion and Implementation	Digital Safety Verification Digital Fault Campaigns	Analog Safety Verification Analog/MS Safety Design and Fault Campaigns
Genus™ Safety Mechanism Insertion	**Verisium™ Safety** Digital Fault Campaign Management	**Virtuoso® Studio** Custom Analog/MS and RF IC Design Platform
Innovus™ Safety Mechanism Implementation	**Jasper® Safety** Fault Pruning and static analysis	**Virtuoso® ADE Assembler** Analog/MS Fault Campaign Management
Conformal® Safety Mechanism Insertional Verification	**Xcelium™ Safety** Concurrent and Serial Fault Simulation	**Virtuoso® ADE Verifier** Analog/MS Verification Cockpit
Cadence Modus DFT Insertion	**Palladium® Safety** Fault Emulation	**Legato®** Fault Simulation and Coverage Analysis
Pegasus™ Physical Safety Checks	**Verisium™ Debug** Fault Debugging and analysis	**Spectre®** Core Simulation Platform

Digital Fault Classification Solution



Implementing Safety Mechanisms (TMR Example)



Synthesis
Inserts voting logic
Protects user-inserted TMR

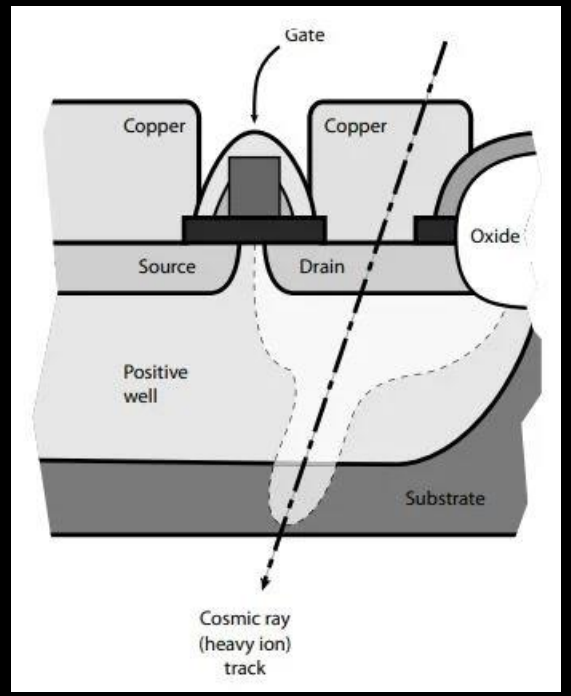
Logic Equivalence
TMR equivalency checks

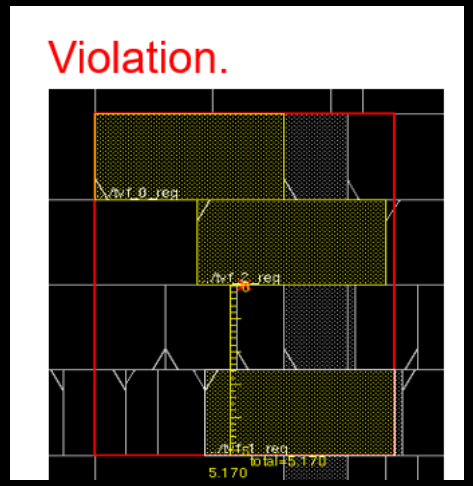
Place and Route
Spacing constraints for flops
Clock isolation

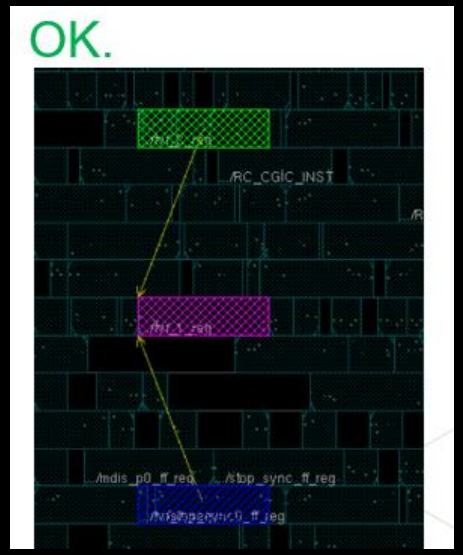
DRC Checks
Checks constraint implementation

Physical Safety Constraints

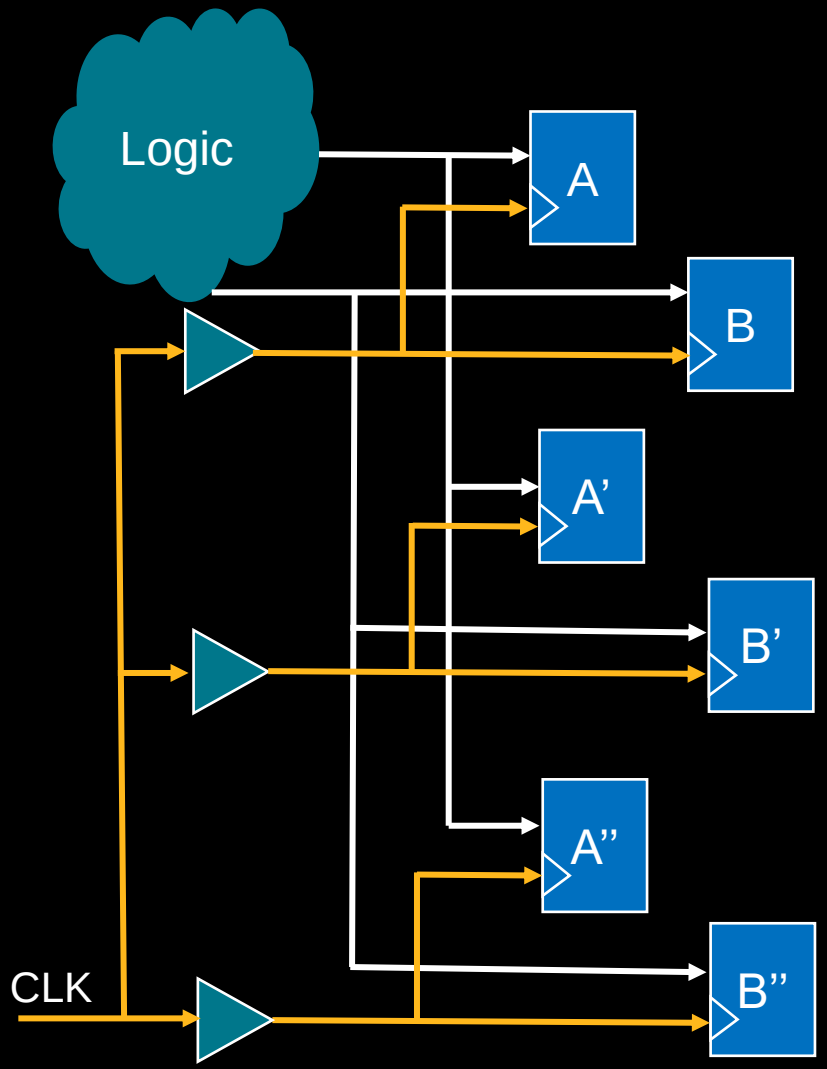
Spacing





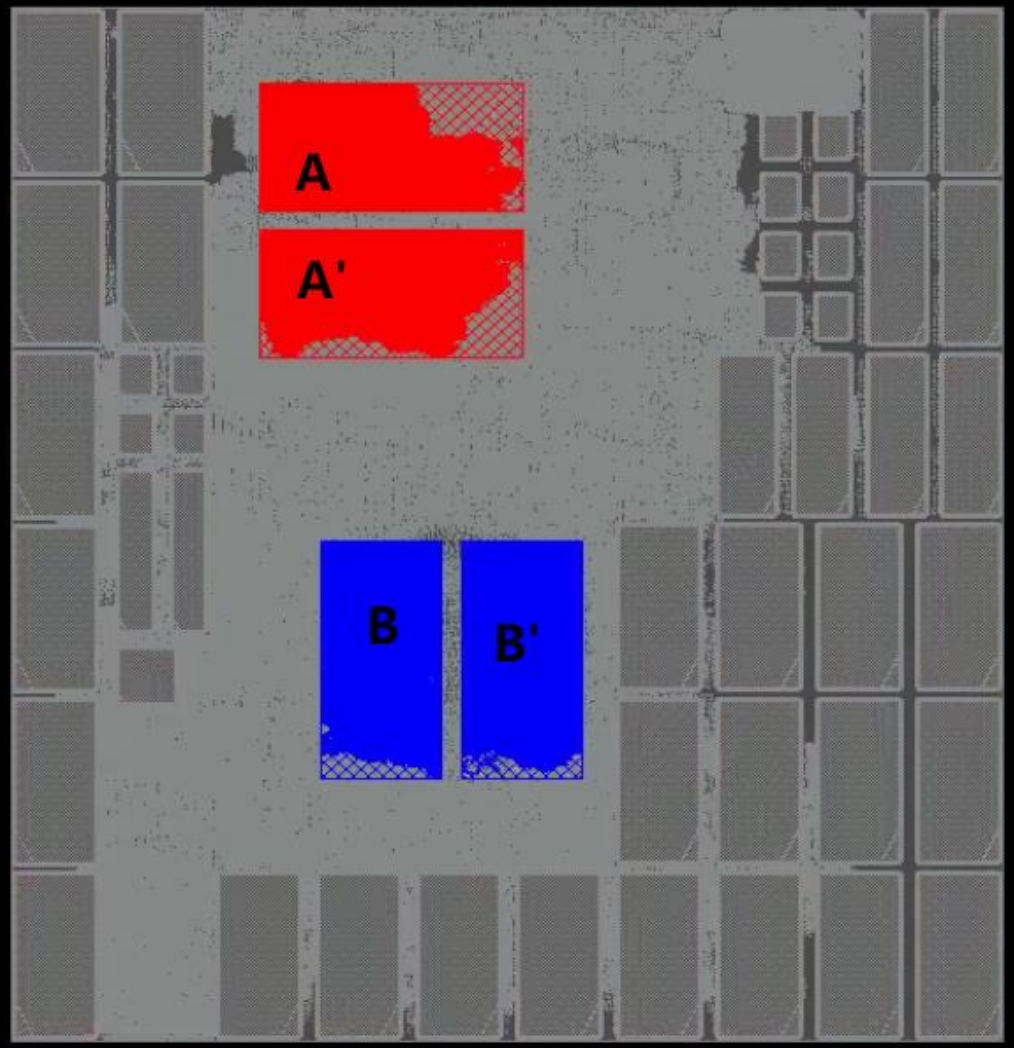


Clock Isolation

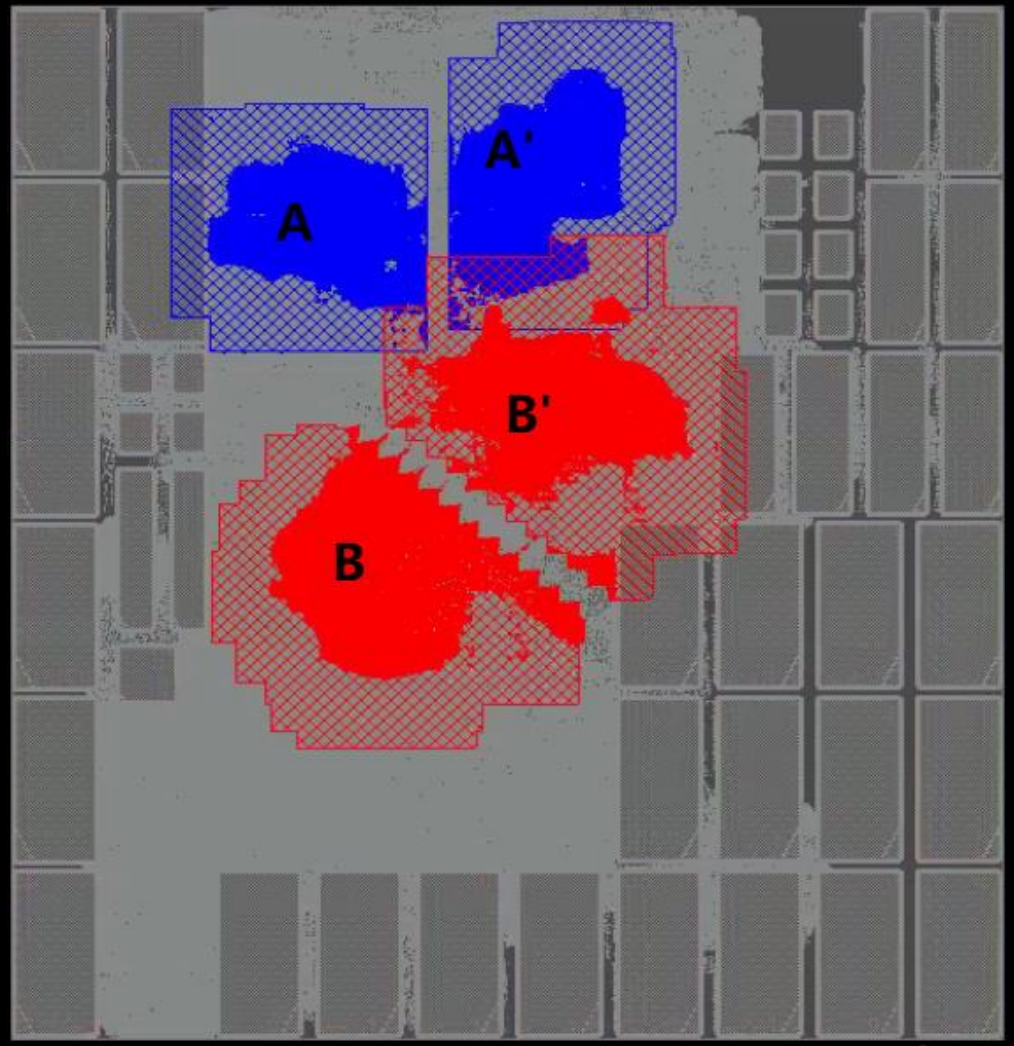


Flexible Region Spacing for Dual-Core Lock Step (DCLS)

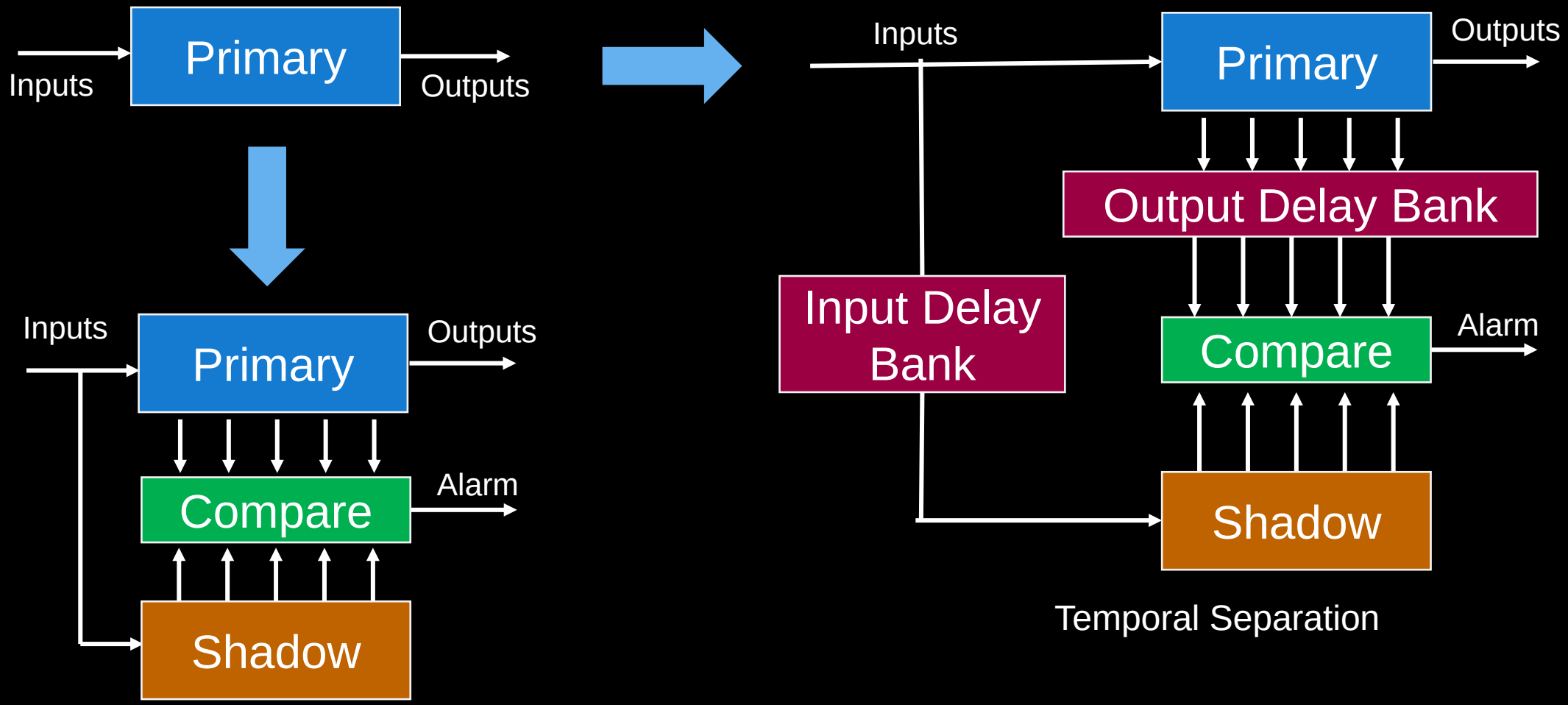
Rectilinear Regions



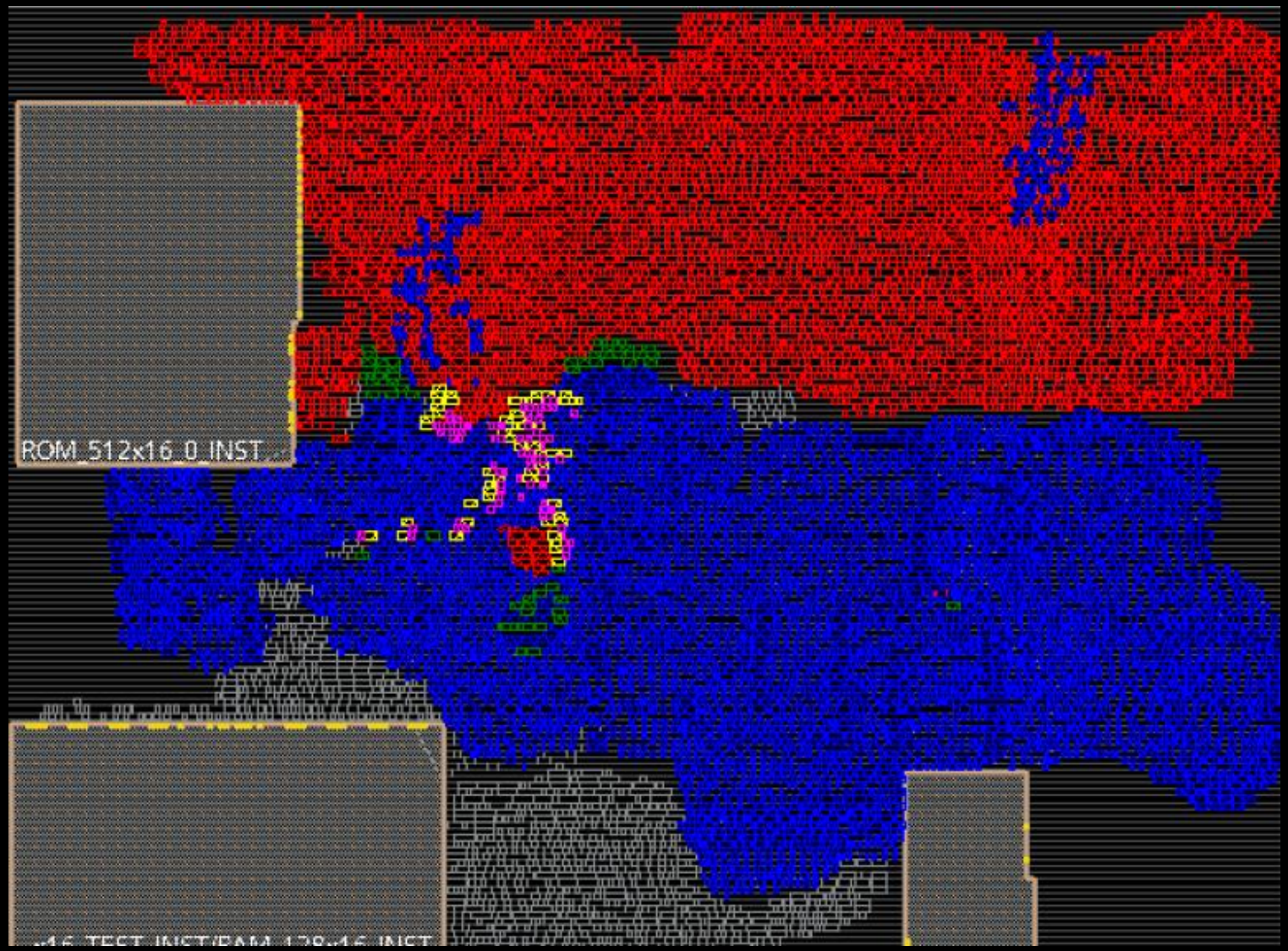
Flexible Region



Hardware Redundancy (Dual-Core Lock Step or DCLS)

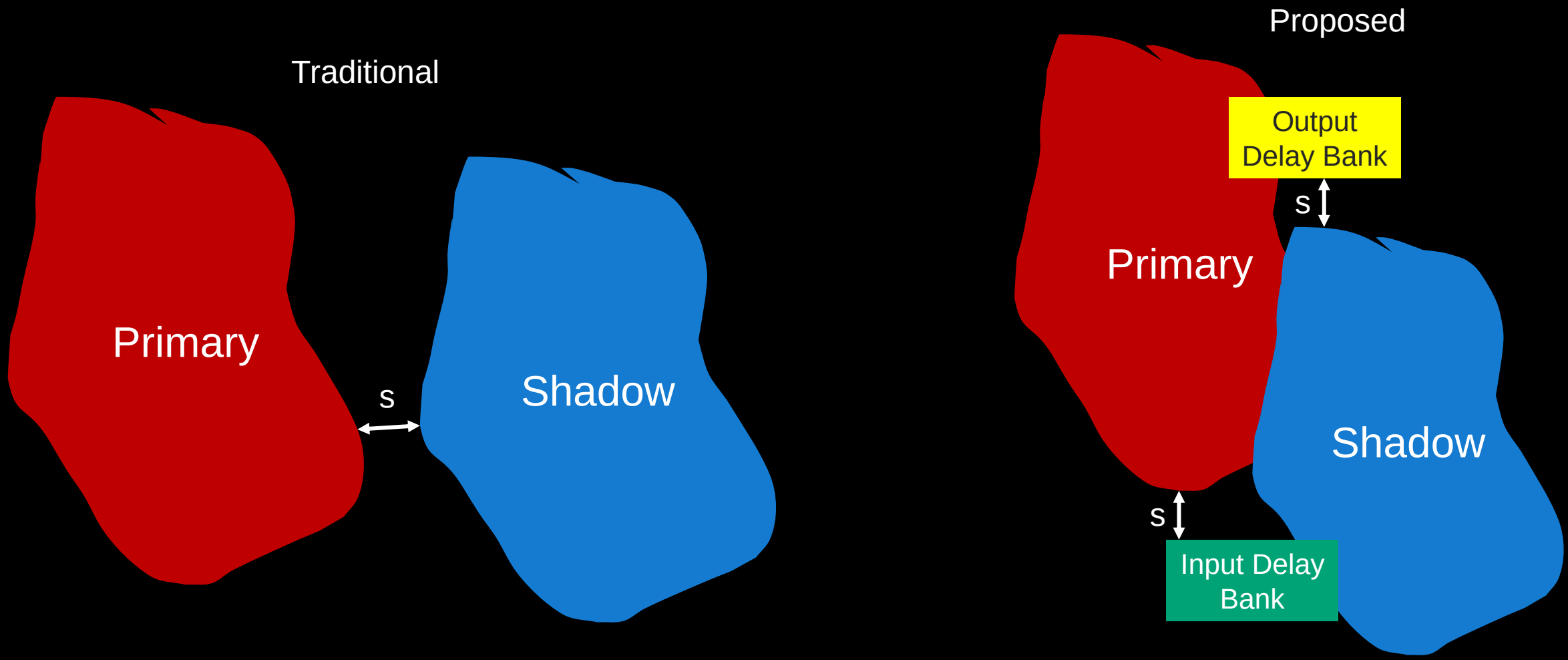


Unconstrained Placement Example



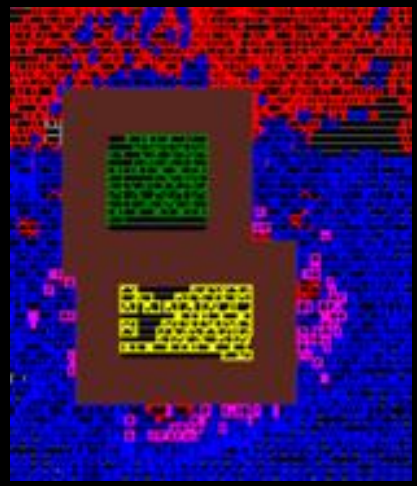
Red: Primary
Blue: Shadow
Green: Input Delay Bank
Yellow: Output Delay Bank
Pink: Compare

Key Idea: DCLS Spacing Constraints

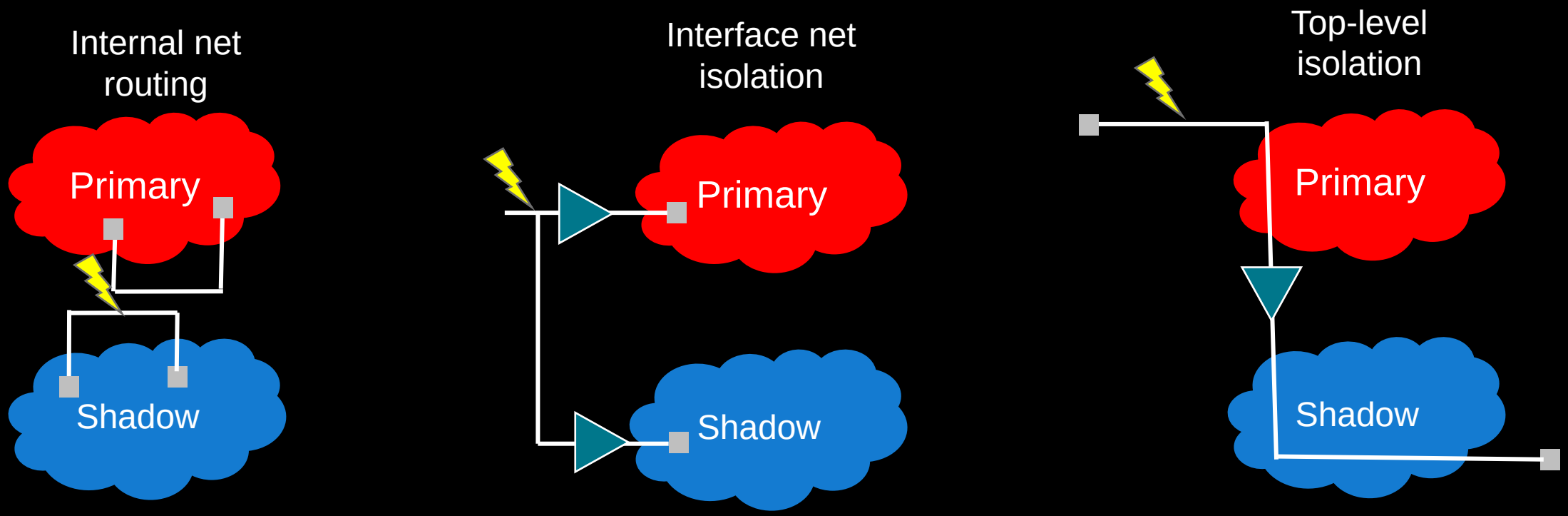


Placement Innovation Required

1. Make delay banks tight and tiny
2. Treat them like floating regions
3. No placement / shadow constraints
4. Create specialized keep-out areas

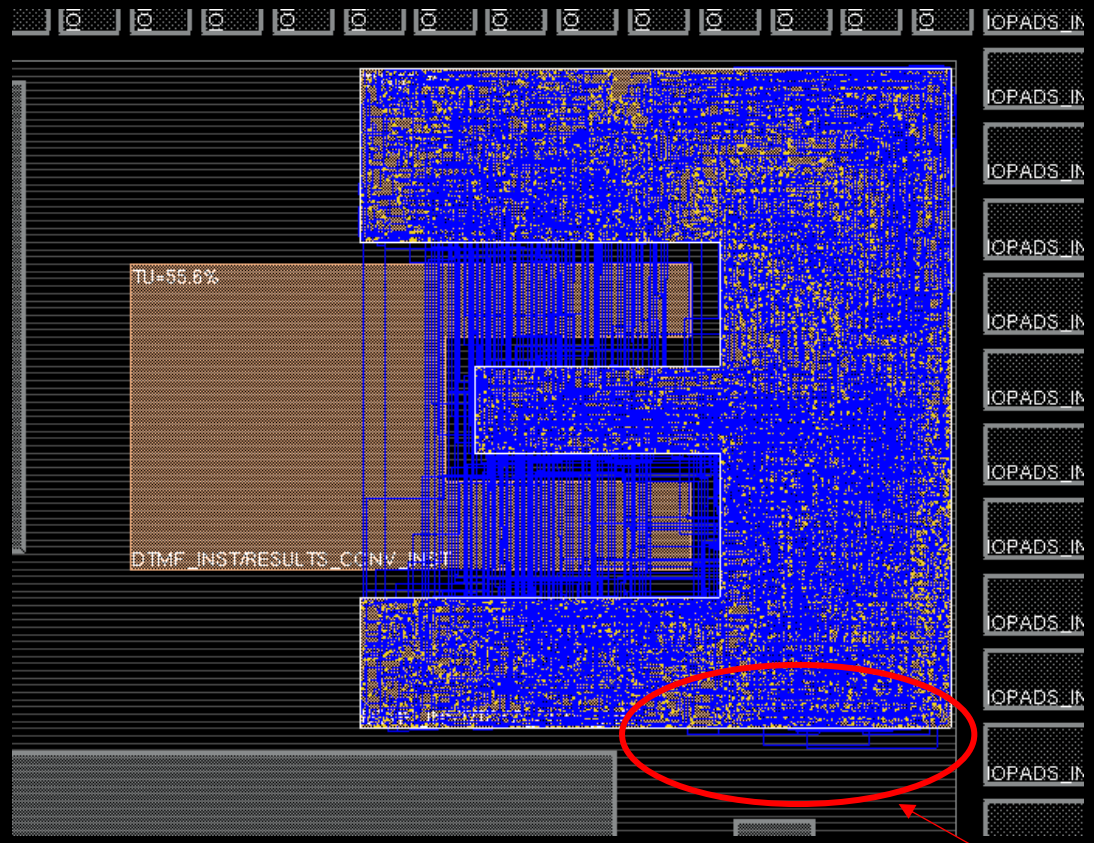


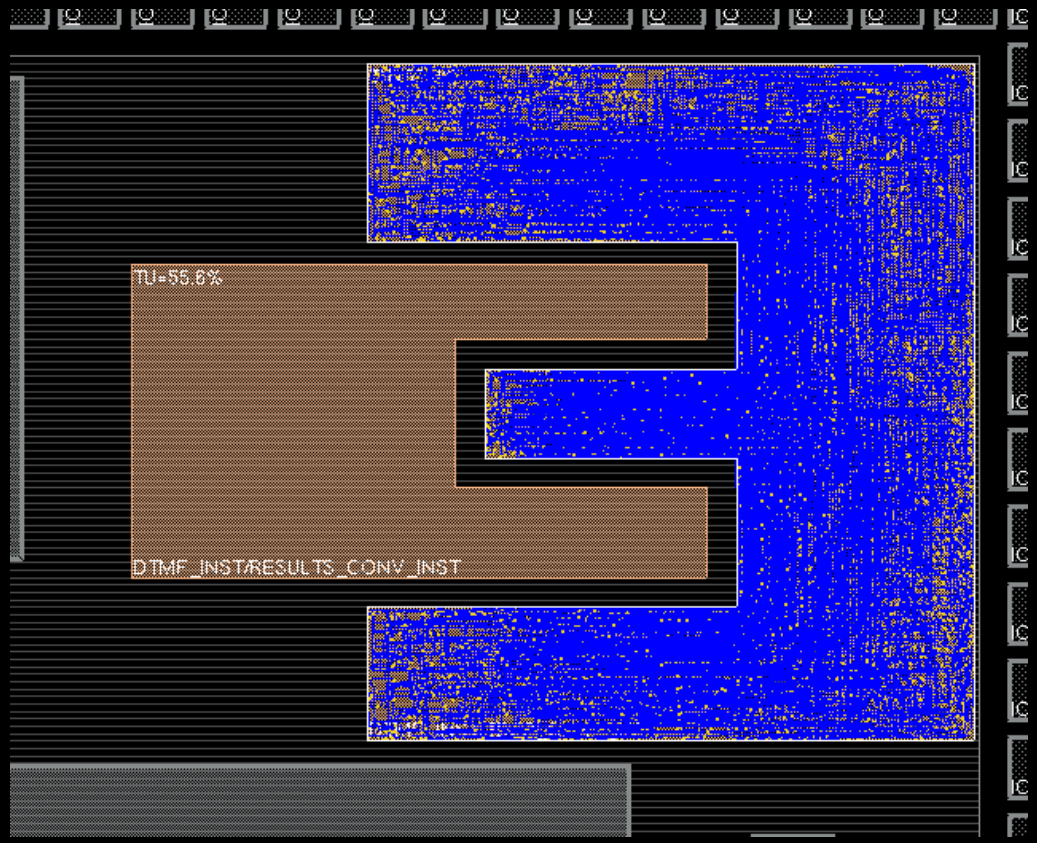
Example Wiring and Buffering Constraints for DCLS



These limitations can be disruptive and distressing
(painful)

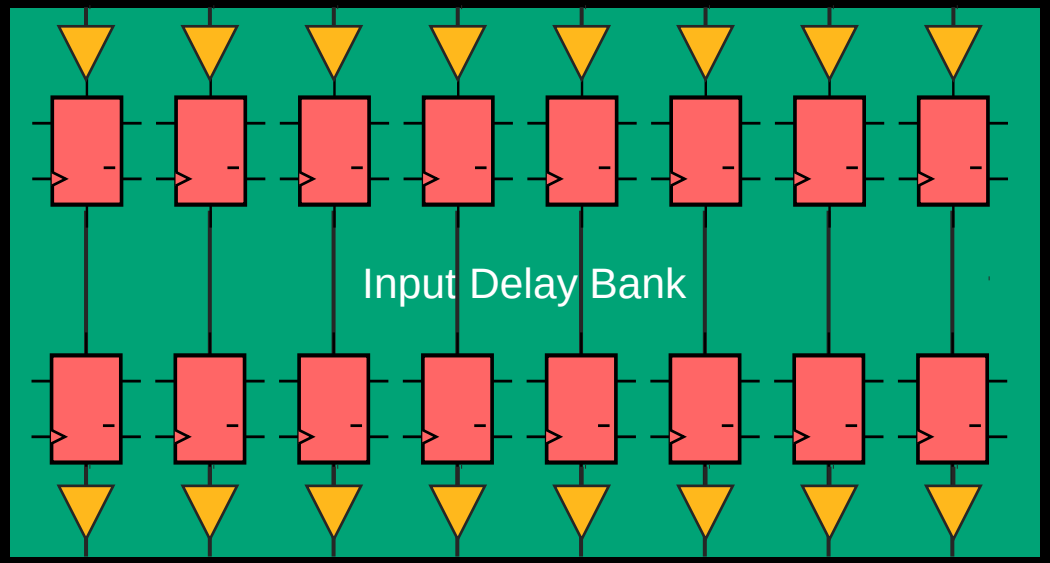
Internal Nets Constraints Example: Overconstrained?





This should be allowed

Handling Routing and Buffering Issues



- Pre-insert small isolation buffers
- All wires in delay bank are super short
- Wire coupling extremely unlikely
- Most buffering / wiring constraints are ignorable

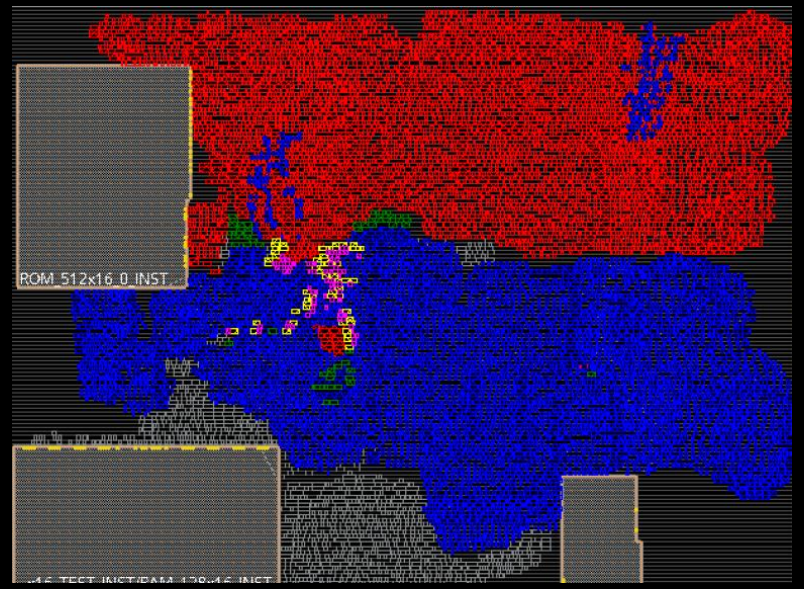
Summary

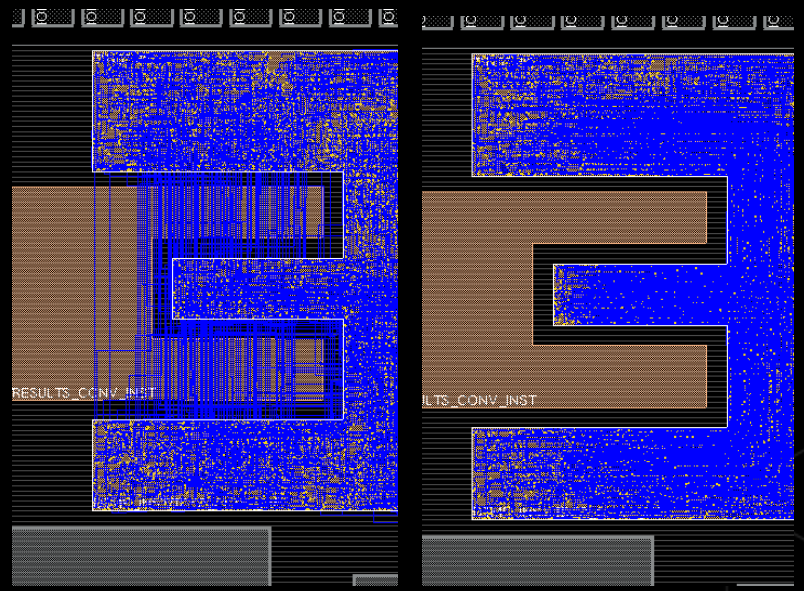
Functional safety mechanisms can occur big design costs

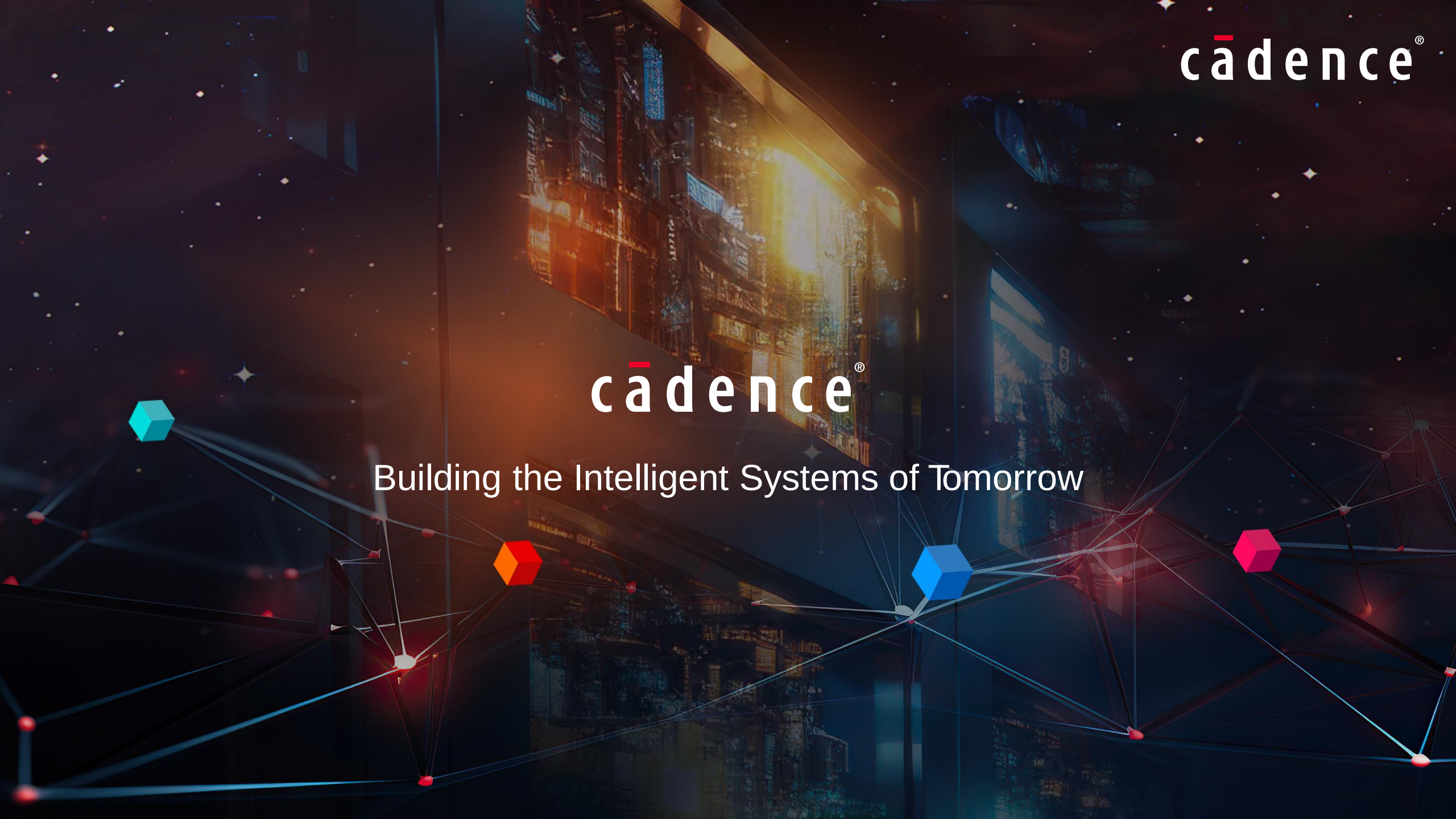
Physical implementation approach matters for PPA

Proposed a new safety case for DCLS

No metric of safety of a physical design






cadence®
cadence®
Building the Intelligent Systems of Tomorrow