Methodology with a formal approach for selective radiation mitigation in space-grade FPGAs

Siemens EDA, IC Verification Solutions

SIEMENS

Agenda

Trends and industry challenges

SEU Analysis Overview

SEU Methodology Overview

SIEMENS

Industry challenges

Current headwinds impacting success

SIEMENS

Challenge 1:
The productivity gap

The widening gap between increasing project complexity and availability (and effectiveness) of talent

SIEMENS

Ever-present productivity gap is growing, with resource deficits predicted

Growth in DV teams, where possible, only slowed the growing gap

DV engineers	Design bugs causing respins	Schedule overruns
↑41%	↑35%	↑5%
Since 2012	*Since 2012*	*Since 2012*

Source: Wilson Research Group and Siemens EDA, 2022 Functional Verification Study

Hardware & software co-development	Compliance amidst customization	Massive-scale interconnect
↑27%	↑30%	↑20%
Since 2016	*Since 2020*	*Since 2020*

Source: Wilson Research Group and Siemens EDA, 2022 Functional Verification Study

Designer demand	Designer supply annual increase	Silicon designer supply gap
↑50%	↑1%	23,000
In 2030 compared to 2022	*Through 2030*	*In 2030*

Source: The Growing Challenge of Semiconductor Design Leadership, Boston Consulting Group & SIA, Nov 2022

Minimal time-to-market impact

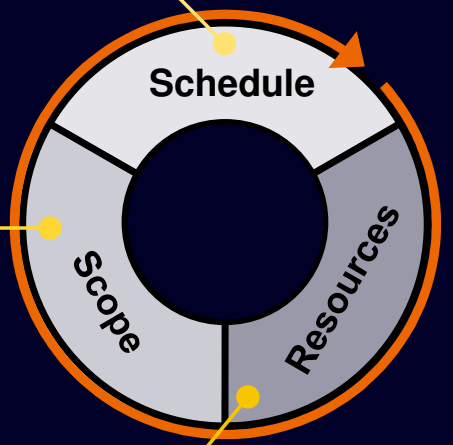
Investing in verification resources did not deliver expected returns

Increasing complexity

Continuing the never-ending trend

Labor shortages

Growing gap of talent emerging from education



SIEMENS

Challenge 2: Hardware assurance

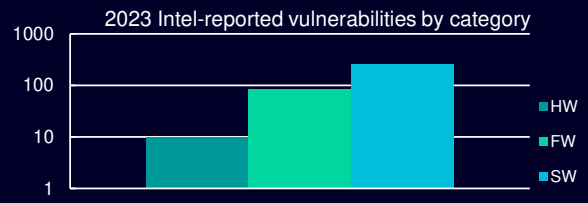
System operational requirements and global environment drive increased assurance scrutiny

SIEMENS

Failure-intolerant applications are increasing in high-vulnerability environment

Current verification methods can not deliver proof of compliance

Hardware vulnerabilities in CPUs and GPUs



https://www.intc.com/news-events/press-releases/detail/1677/intel-releases-2023-product-security-report-highlighting20240223917900/en/

Security and assurance requirements

enisa European Network and Information Security Agency

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

Security features In designs

ASIC	FPGA
↑7.4%	↑13.9%
Since 2020	*Since 2020*

Source: Wilson Research Group and Siemens EDA, 2022 Functional Verification Study

Vulnerabilities

Increased awareness is not eliminating issues

Requirements

New and increasing frequently

Complexity

More features to verify to ensure correct security features in design

Increasing demand for hardware assurance

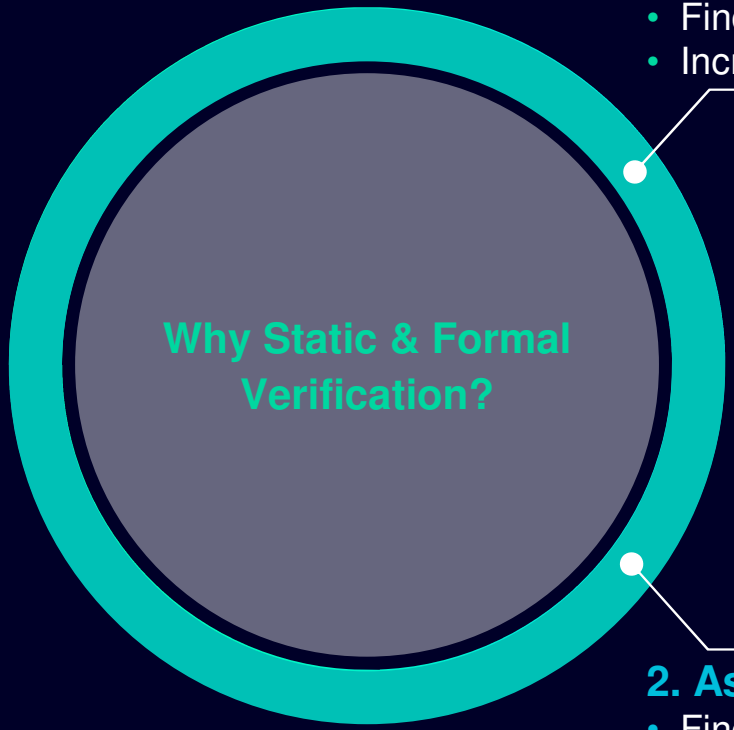
- Supply chain vulnerabilities
- Data confidentiality & integrity
- National Security concerns
- Regulatory requirements
- Growing complexity
- Increased security threats

SIEMENS

Addressing these challenges with Static & Formal technologies

SIEMENS

Static and Formal are critical to success amidst today's industry challenges
Complementary to simulation, deliver assurance and productivity



1. Productivity
- Find issues and get early intent-focused answers
- Increase simulation efficiency with narrower scope and reduced debug

Peak Productivity

Formal First

Absolute Assurance

Proof Positive

2. Assurance
- Find what simulation won't with exhaustive coverage of complete state space

SIEMENS

Questa OneSpin Static & Formal address industry's largest challenges

Complete solution to accelerate productivity & a deterministic path to success

Questa Design Solutions

Automatic Formal for designers and Verification engineers

Increase RTL quality - without a testbench

- Design Checking
- Metastability prevention
- Connectivity Proofs

Questa OneSpin Solutions

Powerful formal verification for critical design functions

Find bugs simulation cannot

- Critical functionalities
- Processor Verification
- Security Validation
- Coverage closure

Questa Equivalent Design

Ensure clean designs remain clean throughout implementation

RTL vs RTL
RTL vs Gate
Verification of ECO changes

SIEMENS

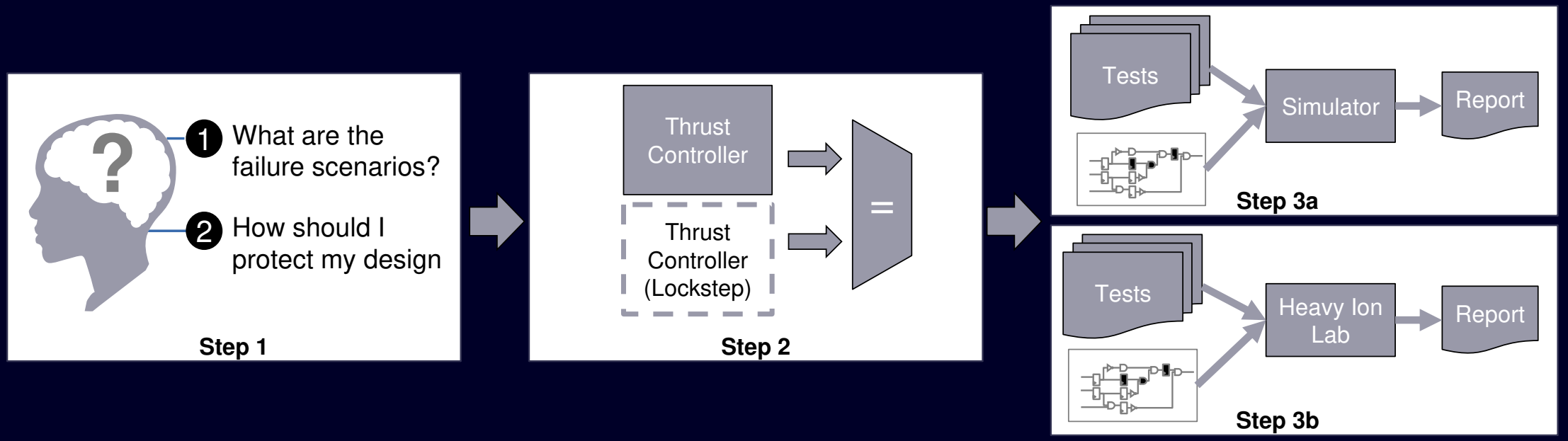
SEU challenges and engine analysis overview

SIEMENS

Common approach to Logical SEU mitigation

Step 1: Failure points are identified through expert driven analysis
Step 2: Insertion of protection is performed by design engineers
Step 3: Verification is commonly performed by (either or both):

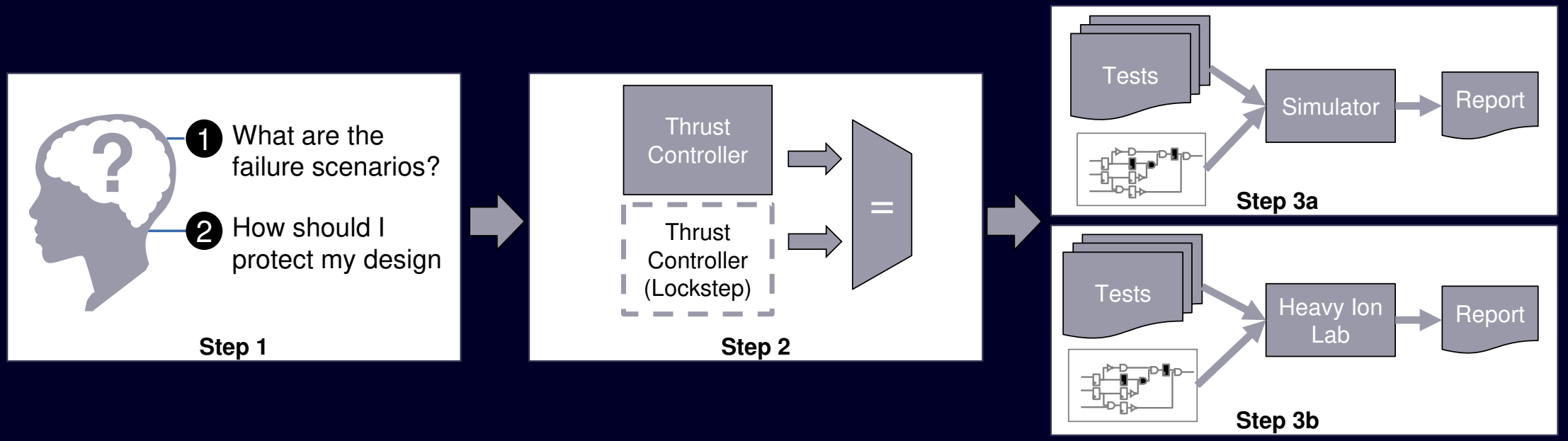
- Simulation leveraging functional regressions and force commands to inject faults
- Functional testing under heavy ion exposure



SIEMENS

Challenges with common approach

1. **Implementation**: Identifying optimal mitigation strategy
2. **Verification**: Delivering quantitative assurance of mitigation effectiveness
3. **Debug**: Visibility and analytics to quickly root cause and fix failures

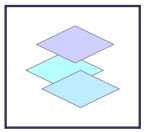


SIEMENS

Logical SEU radiation mitigation platform

1. **Identifies issues** in existing logical radiation mitigation
2. **Classifies unmitigated logic** based on it's potential to affect mission critical functions
3. Provides a **quantitative assessment** of the logical mitigation and generates reports

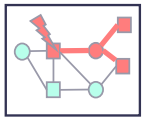
Structural Partitioning



Identify the fault coverage and gaps for hardware mitigation

- Questa Analyze Architecture

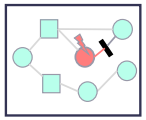
Fault Injection Analysis



Identify the fault coverage and gaps for software mitigation

- Austemper KaleidoScope
- Questa Analyze Fault
- Veloce Fault App

Propagation Analysis



Identify the unprotected faults which can lead to mission failure

- Questa Analyze Architecture
- Austemper KaleidoScope
- Questa Analyze Fault

Metrics Computation

Visualize and report the fault metrics and gaps

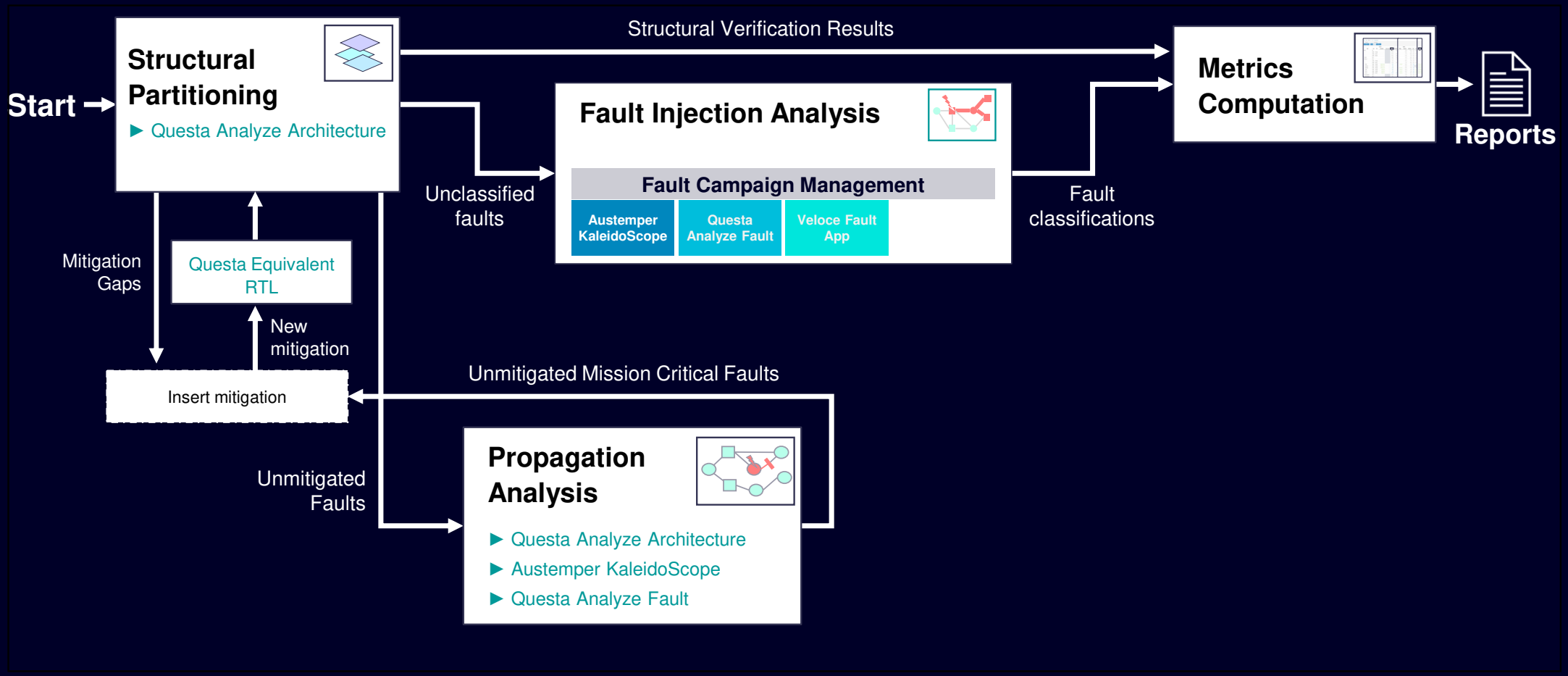
- Proof of Concept

SIEMENS

Logical SEU Mitigation Methodology Overview

SIEMENS

Logical SEU radiation mitigation methodology

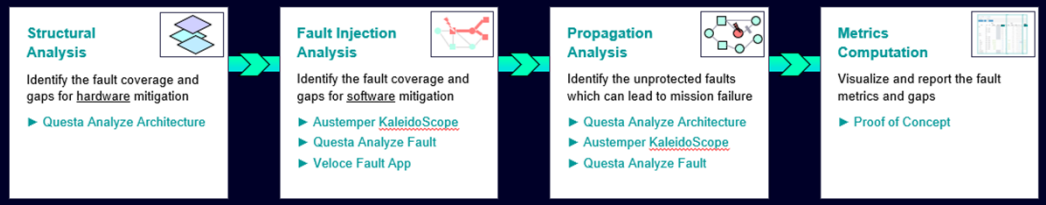


SIEMENS

Conclusion

SIEMENS

Conclusion



Productivity gap is growing. Complexity is increasing

- Teams need to adopt more advanced verification techniques
- Static & Formal can help both in finding bugs earlier, and in finding bugs other solutions cannot

This proposed methodology

- Provides a quantitative assessment of the effectiveness of SEU mitigation strategies
- Highlights existing gaps and unprotected logic
- Leverages Siemens' static and formal verification technologies, to achieve absolute assurance and increased productivity in addressing these critical hardware reliability challenges.

SIEMENS

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Contact

Published by Siemens

Mark Handover
Application Engineer

E-mail mark.handover@siemens.com

SIEMENS