Universität Stuttgart
Institute of Computer Architecture and Computer Engineering

DFG Deutsche Forschungsgemeinschaft

ITI

GS-IMTR
Graduate School
Intelligent Methods for Test and Reliability

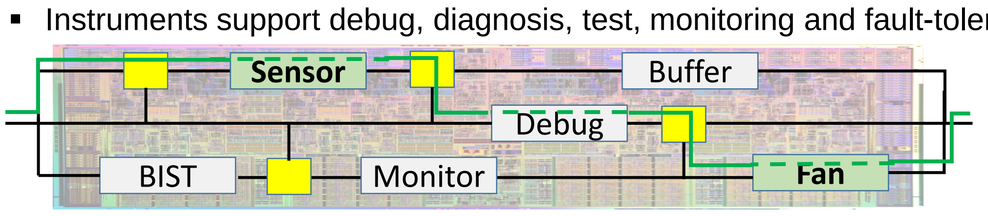
Dependable Reconfigurable Scan Networks
Analysis and Resynthesis

Natalia Lylina • Hans-Joachim Wunderlich

Need for reconfigurable scan networks (RSNs)

Dependable systems integrate an extensive number of embedded instruments:

- Instruments support debug, diagnosis, test, monitoring and fault-tolerance



- **Example**: **Temperature sensor** in a processor detects increased temperature. The cooling system adjusts the speed of a **fan** to decrease the temperature.

RSNs flexibly access the instruments through a scan path (in green):

- Collect the evaluation results
- Control (runtime-adaptive) instruments
- Perform online health monitoring
- Guide fault-handling

Scan segments (in yellow) control the scan path or act as an interface to on-chip instruments.

- Access through atomic operation of three phases: Capture, Shift, Update

Threats due to the improper RSN integration

Faults in the RSN:
- Inaccessible RSN parts
- Inaccessible instruments

Undetected faults in the RSN:
- Silent data corruption

Extra connectivity due to the RSN:
- Unauthorized access
- Sensitive data leakage

→ **System failure** or **permanent damage**

Challenges of dependable RSNs

RSNs are inherently sequential with high depth

- Single shift-in/out operation can take thousands of cycles

Access to a target register may require multiple reconfigurations:

- Combinational dependencies of the control logic
- Sequential dependencies of the scan cells

Conventional cycle-accurate models and algorithms lack scalability

Dependable RSNs: A complete approach

Robust RSNs

To ensure reliable access via RSNs, the overall damage in the presence defects in the RSN must be minimized:

- **State-of-the-art**: Fault-tolerance requires diagnostic support and complicates routing

Our solution [7]: **Fault-avoidance** reduces probability of fault activation; the RSN structure is unchanged – access pattern compatibility:

1. Precise RSNs **criticality analysis:**
   - Custom damage weights show the instruments' relevance
   - Influence of an RSN defect on an observability/setability of instruments

2. Selective **RSN hardening** against permanent faults:
   - **Post-silicon validation**: major part are accessible
   - **Runtime**: the most critical instruments are accessible
   - Evolutionary algorithms formulation:
     Hardware cost vs. resilience

Testable RSNs

Testability of control lines: Correctness of a path through the RSN must be testable:

- **State-of-the-art** methods only detect those faults, which alter the current path length.

Our solution [6]**:**

1. Precise **testability analysis**:
   - All single faults detectable by an altered path length?

No!

2. Light-weight **testability-enhancing resynthesis**:
   - A small number of cells is added to ensure unique path lengths for single faults

All single faults in the control logic are detectable.

Scan integrity test: Integrity of the current path is tested by a short pre-sequence concurrently to other tasks [5].

Security Compliant RSNs

Unwanted extra-connectivities in the system due to improper RSN integration must be avoided:

- **State-of-the-art** does not scale due to the RSN complex control dependencies and high sequential depth

Our solution [9]:

1. Precise **security compliance analysis** [2]:
   - Identify the violations as additional unwanted connectivities due to RSN integration

2. Efficient **security-preserving resynthesis** [3]:
   - Resolve all the violations with minimized structural changes
   - Preserve the accessibility of the instruments via RSNs

3. Flexible **multi-user protection** [4]:
   - Consider the user-specific access requirements
   - Minimize the hardware costs even more
   - Still guarantee the required accessibility

Conclusions

To support dependable system operation, dependability threats due to the **RSN** integration must be mitigated, e.g.:

- Faults in the RSNs must be tested and, if possible, avoided
- Information leakage must be mitigated

This dissertation presents dependable RSNs for the whole system **lifecycle**:

- Guarantee **robust access** to instruments via RSNs
- Ensure **fault detection** in RSNs
- Avoid undesired **extra connectivities** due to RSNs

By the means of:

- Precise and scalable **analysis** of **RSN dependability properties**
- Automated **resynthesis** of **dependable RSN**

Publications

Peer-reviewed conferences and journals:

[1] Pascal Raiola, Benjamin Thiemann, Jan Burchard, Ahmed Atteya, **Natalia Lylina**, Hans-Joachim Wunderlich; Bernd Becker and Matthias Sauer, "On Secure Data Flow in Reconfigurable Scan Networks ", In Proc. of the Conf. on Design, Automation and Test in Europe (DATE), 2019

[2] **Natalia Lylina**, Ahmed Atteya, Pascal Raiola, Matthias Sauer, Bernd Becker and Hans-Joachim Wunderlich, "Security Compliance Analysis of Reconfigurable Scan Networks", In Proc. of the IEEE International Test Conference (ITC), 2019

[3] **Natalia Lylina**, Ahmed Atteya, Chih-Hao Wang, and Hans-Joachim Wunderlich, "Security Preserving Integration and Re-Synthesis of Reconfigurable Scan Networks". In Proc. of the IEEE International Test Conference (ITC), 2020

[4] **Natalia Lylina**, Ahmed Atteya, and Hans-Joachim Wunderlich, "A Hybrid Protection Scheme for Reconfigurable Scan Networks", In Proc. of the VLSI Test Symposium (VTS), 2021

[5] Chih-Hao Wang, **Natalia Lylina**, Ahmed Atteya, Tong-Yu Hsieh and Hans-Joachim Wunderlich, "Concurrent Test of Reconfigurable Scan Networks for Self-Aware Systems", In Proc. of the IEEE International Symp. on On-Line Testing and Robust System Design (IOLTS), 2021

[6] **Natalia Lylina**, Chih-Hao Wang and Hans-Joachim Wunderlich, "Testability-Enhancing Resynthesis of Reconfigurable Scan Networks", In Proc. of the IEEE International Test Conference (ITC), 2021

[7] **Natalia Lylina**, Chih-Hao Wang and Hans-Joachim Wunderlich, "Robust Reconfigurable Scan Networks", In Proc. of the Conf. on Design, Automation and Test in Europe (DATE), 2022

[8] Hussam Amrouch, Jens Anders, Steffen Becker, Maik Betka, Gerd Bleher, Peter Domanski, Nourhan Elhamawy, Thomas Ertl, Athanasios Gatzastras, Paul R. Genssler, Sebastian Hasler, Martin Heinrich, André van Hoorn, Hanieh Jafarzadeh, Ingmar Kallfass, Florian Klemme, Steffen Koch, Ralf Küsters, Andrés Lalama, Raphael Latty, Yiwen Liao, **Natalia Lylina**, Zahra Paria Najafi-Haghi, Dirk Pflüger, Ilia Polian, Jochen Rivoir, Matthias Sauer, Denis Schwachhofer, Steffen Templin, Christian Volmer, Stefan Wagner, Daniel Weiskopf, Hans-Joachim Wunderlich, Bin Yang and Martin Zimmermann, "Intelligent Methods for Test and Reliability", In Proc. of the Conf. on Design, Automation and Test in Europe (DATE), 2022

[9] **Natalia Lylina**, Chih-Hao Wang and Hans-Joachim Wunderlich, "SCAR: Security Compliance Analysis and Resynthesis of Reconfigurable Scan Networks", Accepted for publication in the IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 2022

Contact: lylina@informatik.uni-stuttgart.de

ITI