CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

# Proceedings of the 11th Prague Embedded Systems Workshop

June 29 - July 1, 2023

Horoměřice
Czech Republic

ISBN 978-80-01-07178-6

Editors:

prof. Ing. Hana Kubátová, CSc.
doc. Ing. Petr Fišer, Ph.D.
Ing. Jaroslav Borecký, Ph.D.

# Message from the Program Chairs

The Prague Embedded Systems Workshop is a research meeting intended for the presentation and discussion of students' results and progress in all aspects of embedded systems design, testing, and applications. It is organized by members of the Department of Digital Design at the Faculty of Information Technology and supported by the Czech Technical University in Prague. The workshop focuses mainly on new technologies and methods, dependable and low power design, and it also has a special session on network security under the auspices of the Network Traffic Monitoring Lab. The workshop aims to enhance collaboration between different universities not only inside the EU. It is based on oral presentations, mutual communication, and discussions.

There are three types of students' submissions and presentations:

- Full papers describing the students' original research. These papers were submitted to a standard reviewing process.
- Abstracts of authors' earlier published and successfully presented papers (at conferences, journals, etc.). These contributions were not reviewed; emphasis was put on the presentation and discussion.
- Student posters - abstracts of defended Bc. and MSc. theses with subsequent poster presentation. This workshop session is traditionally organized as a contest sponsored by IEEE and industry.

Nine papers were accepted for PESW 2023 oral presentation, from which there was one full paper and eight abstracts. Contributions from Austria, Germany, Israel, and Czech Republic were accepted this year.

The technical program is also highlighted by two keynote speakers:

- Approximate computing in neural networks.
  *Speaker:* Vojtěch Mrázek, Brno University of Technology, Czech Republic
- Resilient RISC-V processor for aerospace applications: from on-chip sensors to AI-based reliability prediction.
  *Speaker:* Fabian Vargas, IHP - Leibniz Institute for High Performance Microelectronics, Germany

PESW 2023 program contains four Technical sessions, the Poster sessions with IEEE contest and five Industrial talks.

We would like to thank to our sponsors CTU in Prague, Research Center for Informatics, ASICentrum, CISCO, STMicroelectronics, SYSGO, IMA, METIO Software, Institute for Support of Innovative Education.
Special thanks go to IEEE: IEEE Student Branch at Czech Technical University in Prague and IEEE Young Professionals, organizing student contest, and Czechoslovakia Section of IEEE.

We wish the 11th Prague Embedded System Workshop many heated discussions and possible establishment of mutual research collaboration.

Hana Kubátová and Petr Fišer
29th June 2023

# Committees

## Workshop Chairs

Hana Kubátová, CTU in Prague (CZ)

Petr Fišer, CTU in Prague (CZ)

## Programme Committee

J. Bělohoubek, CTU in Prague, FIT (CZ)

A. Bosio, École Centrale de Lyon (FR)

L. Cassano, Politecnico di Milano (IT)

T. Čejka, CTU in Prague (CZ)

G. DiNatale, TIMA, Grenoble (FR)

R. Drechsler, University of Bremen (DE)

P. Fišer, CTU in Prague, FIT (CZ)

J.L. Gaudiot, University of California, Irvine (USA)

K. Jelemenská, STU Bratislava (SK)

M. Jenihhin, Tallinn Univ. of Technology (EE)

P. Kitsos, TEI West. Greece (GR)

M. Krstić, IHP, Frankfurt (Oder) (DE)

H. Kubátová, CTU in Prague, FIT (CZ)

R. Kvaček, ASICentrum, Prague (CZ)

F. Leporati, Univ. di Pavia (GR)

I. Levin, Tel-Aviv University (IL)

R. Lórencz, CTU in Prague, FIT (CZ)

A. McEwan, University of Leicester (UK)

N. Mentens, KU Leuven (BE)

P. Mróz, University of Zielona Gora (PL)

M. Novotný, CTU in Prague, FIT (CZ)

A. Orailoglu, UC San Diego (USA)

Z. Plíva, TU Liberec (CZ)

M. Poupa, University of West Bohemia, FEE (CZ)

J. Schmidt, CTU in Prague, FIT (CZ)

M. Skrbek, CTU in Prague, FIT (CZ)

J. Sobotka, CTU in Prague, FEE (CZ)

B. Steinbach, TU Chemnitz (DE)

A. Steininger, Vienna University of Technology (AT)

Z. Vašíček, Brno University of Technology, FIT (CZ)

W. Zając, Jacob of Paradies University (PL)

## Special Session on Network Security Chair

Tomáš Čejka, CTU in Prague (CZ)

## Student Poster Session Co-Chairs

Tomáš Kolárik, CTU in Prague (CZ)

Jaroslav Pešek, CTU in Prague (CZ)

## Organizing Committee

H. Kubátová, CTU in Prague (CZ)

P. Fišer, CTU in Prague (CZ)

J. Borecký, CTU in Prague (CZ)

M. Novotný, CTU in Prague (CZ)

R. Kinc, AMCA (CZ)

E. Uhrová, AMCA (CZ)

# Contents

# Keynotes

## Resilient RISC-V processor for aerospace applications: from on-chip sensors to AI-based reliability prediction

Speaker: **Fabian Vargas**, *IHP - Leibniz Institute for High Performance Microelectronics, Germany*

Technology scaling, which made electronics accessible and affordable for almost everyone on the globe, has advanced integrated circuit (IC) and electronics since the sixties. Nevertheless, it is well recognized that such scaling has introduced new (and major) reliability challenges to the semiconductor industry.

This talk describes the on-chip infrastructure such as sensors and dedicated HW redundancy under development at IHP Microelectronics. This infrastructure deals with, for instance, detecting single-event upset (SEU) in memory elements and single-event transient (SET) in logic, measuring electronics aging during IC lifetime, and ultimately predicting in-flight SEU rate and remaining IC life-span. Dedicated on-chip watchdogs to guarantee mixed-criticality task execution in real-time operating system (RTOS) is further introduced.

Currently, this on-chip infrastructure is being implemented by IHP in different versions of a quad-core RISC-V processor. This IC has been designed by using a CMOS 130nm rad-hard technology also developed at IHP. An FPGA-mapped demonstrator of the developed RISC-V processor and experimental results will be presented and discussed.

**Fabian Vargas**

Fabian Vargas obtained the Ph.D. Degree in Microelectronics from the Institut National Polytechnique de Grenoble (INPG), France, in 1995. At present, he is Senior Scientist at IHP - Leibniz Institute for High Performance Microelectronics, Germany, where he works on on-chip sensors and cross-layer resilience for aerospace-application systems. Vargas has served as Technical Committee Member and Guest-Editor in many IEEE-sponsored conferences and journals. He holds several patents and published over 200 refereed papers. Vargas was researcher of the BR National Science Foundation from 1996 to 2023. He co-founded the IEEE-Computer Society Latin American Test Technology Technical Council (IEEE LA-TTTC) in 1997 and the IEEE Latin American Test Symposium (LATS) in 2000. He received for several times the Meritorious Service Award of the IEEE Computer Society for providing significant services as chair of these groups. Vargas is Golden Core Member of the IEEE Computer Society and Senior Member of the IEEE.

## Approximate computing in neural networks

Speaker: **Vojtěch Mrázek**, *Brno University of Technology, Faculty of Information Technology, Czech Rep.*

Neural networks and their accelerators appear in many embedded applications that are power constrained. One way to reduce the power consumption of these networks without significantly changing the architecture is to exploit the benefits of approximate computing. This approach exploits the fact that users are willing to accept some error at the cost of lower energy consumption. In this keynote, approaches for the controlled introduction of error into the computational path will be presented. It will be demonstrated approaches for an error-resilience evaluation and for an efficient mapping of layers to approximation components.

**Vojtěch Mrázek**

Vojtěch Mrázek received a M.Sc. and Ph.D. degrees in information technology from the Faculty of Information Technology, Brno University of Technology, Czech Republic, in 2014 and 2018. He is a assitant professor at the Faculty of Information Technology with Evolvable Hardware Group and he was also a visiting post-doc researcher at Institute of Computer Engineering, Technische Universität Wien (TU Wien), Vienna, Austria (2018-2019). His research interests are approximate computing, genetic programming and machine learning. He has authored or co-authored over 45 conference/journal papers focused on approximate computing and evolvable hardware. He received several awards for his research in approximate computing, including the Joseph Fourier Award in 2018 for research in computer science and engineering.

# Industrial Talks

## Economically self-sufficient education of software development

Speaker: **Tomáš Martinec**, *Institute for Support of Innovative Education, Czech Republic*

The talk briefly introduces activities of the Institute and then presents outcomes of its internal project of innovating software development education for high-school level students. The students engage in real-world software development tasks with support of mentors or their peers. This way they develop their software development skills in a very fast manner, many times even able to develop enough code of value that it covers almost wholly the expenses of this approach to education.

**Tomáš Martinec**

Studied computer science at the Faculty of Mathematics and Physics, Charles University, Prague. Currently, the managing partner of the Institute for Support of Innovative Education. His main domain there is industrial or technology education and secondary-level education. He is also a verification engineer in Sysgo for almost 10 years where he verifies that safety-critical software works as expected. Besides that in Sysgo he trains newcomers as a company tutor and coordinates cooperation with local universities. Two years ago he founded Metio Software s.r.o. and nowadays he engages in two more enterprises in physiotherapy and cybersecurity. In September 2022 he also became a uni lecturer in operating systems programming.

## Enhancing connectivity with I3C

Speaker: **Adam Berlinger**, *STMicroelectronics, Czech Rep.*

I3C is a serial communication interface developed by the MIPI® Alliance that aims to improve and overcome limitations of the well-established I2C. It allows achieving higher data rates, improving power efficiency and reducing signal count. Since the standard is developed by the MIPI® Alliance and is partially open, we might see broader adoption in near future.
This presentation gives a brief overview on how the I3C bus works, how it is compatible with I2C and what are its main advantages. We will have a look on different transfers occurring on the bus as well as some advanced features.

**Adam Berlinger**

Adam Berlinger studied Open Informatics at Faculty of Electrical Engineering at Czech Technical University. He has been working at STMicroelectronics since 2014 as a technical support engineer for STM32 microcontrollers, focusing on high-performance families and communication protocols.

## Risk-based access control system

Speaker: **Tomáš Trpišovský**, *IMA s.r.o., Czech Rep.*

Traditional (physical) access control systems are well-established mechanisms, allowing organizations to determine who should be able to access which physical space. During the Covid-19 pandemic, additional features to the reduce the risks of individuals when entering spaces became popular or even mandatory. We refer to this as risk-based access control (RiBAC). For instance, automatic scanning for protective wear (e.g., whether an individual wears a mask), body temperature checks or digital health certificates, certifying that one has been negatively tested for, or vaccinated against, Covid-19.
In this context, we discuss the use of privacy-preserving cryptography in order to be able to have privacy-preserving risk-based access control systems in place for any potential future pandemic.

**Tomáš Trpišovský**

Tomas Trpisovsky is founder of Institute of Microelectronic Applications (IMA) located in Prague. Established in 1992, IMA became one of leading innovative and proactive and internationally recognized Czech SME. In Jan 2021 IMA has been acquired as R&D center by German WITTE Automotive GmbH and thus became a Large Enterprise. Tomas participated on incubation of international activities, like eEurope Smart Card Charter, EFMI (European Federation of Medical Informatics), MasterCard Vendor Information Forum (GVIF – banking). Since 2008 is active within AENEAS and ARTEMISIA JU and its successors in order to ensure international collaboration, harmonization and interoperability. 2006 - 2017 representative of the Czech Republic in ISO JTC1 SC17 and CEN TC224. 2003 - 2005 co-chair of EFMI WG Card, focused on smart card applications in health care across Europe 2001 - co-founder and technical director of Connectivit-E, hi-tech VA (US).

## Is a Matter future of Smart homes?

Speaker: **Jiří Vlček**, *STMicroelectronics, Czech Rep.*

The goal of the Matter project is to simplify development for manufacturers and increase compatibility for consumers with a unified connectivity protocol. Matter is an application layer protocol using existing technologies such as Thread, Wifi, Ethernet and BLE. The main idea of the Matter is to have only one Gateway and one Smart phone app at home to control all the devices around - no matter who is vendor of the device. By building upon Internet Protocol (IP), the project aims to enable communication across smart home devices, mobile apps, and cloud services and to define a specific set of IP-based networking technologies for device certification.

**Jiří Vlček**

Jiří Vlček is an Application Engineer in STM32 support team and is focused on Wireless applications including BLE, Thread and Matter. Jiri joined STMicroelectronics in 2016 and previously studied at Czech Technical University in Prague.

## Comprehensible multi-modal detection of cyber threats

Speaker: **Martin Kopp**, *CISCO*

Detection of malicious activities is a very complex task and much effort has been invested into research of its automation. However, vast majority of existing methods operate only in a narrow scope which limits them to capture only fragments of the evidence of malware's presence. Consequently, such approach is not aligned with the way how the cyber threats are studied and described by domain experts. In this talk, we discuss these limitations and design a detection framework which combines observed events from different sources of data. Thanks to this, it provides full insight into the attack life cycle and enables detection of threats that require this coupling of observations from different telemetries to identify the full scope of the incident. We demonstrate applicability of the framework on a case study of a real malware infection observed in a corporate network.

**Martin Kopp**

Martin Kopp received PhD in Informatics from the Faculty of Information Technology, Czech Technical University in Prague, in 2019. He worked for two years at the Academy of Sciences of the Czech Republic. Currently, he works for CISCO as Data Science Leader at TD&R Data Science department in Prague. His research interests include multi-modal analytics, comprehensible classification, outlier explanation, and design and breaking of human interaction proves such as CAPTCHA.

# Surveying the security of access systems in Uppsala and Birmingham

Tomáš Přeučil, Martin Novotný
*Faculty of Information Technology*
*Czech Technical University in Prague*
Thákurova 9, 160 00 Praha, Czech Republic
{tomas.preucil — martin.novotny}@fit.cvut.cz

### Abstract

Today, many people use several access systems on a daily basis without paying attention to the fact that many of the technologies in use are obsolete and insecure. For example, there are published attacks against all generations of MIFARE Classic cards and cloning a MIFARE Ultralight card is trivial. In this work, we look into the security of several access systems in a student town Uppsala in Sweden. We also compare these systems to the access system of the University of Birmingham.

We evaluate the security of the cards or tags used for access as well as some of the security of the systems themselves. We present a detailed report on the configurations, including any vulnerabilities, while also presenting attacks exploiting these vulnerabilities, as well as real-life examples of how these attacks can be dangerous to the end user.

We compare these systems to a well-designed system in the same city and suggest fixes for all vulnerabilities we found. When presenting the potential fixes, we pay attention to the ease and cost of the fixes.

***Keywords*— security, cryptanalysis, attacks, access systems, RFID, MIFARE Classic, MIFARE DESFire**

### Acknowledgment

This work and related travel expenses were co-financed by the European Union within the project ”Mobility CTU - STA”, project registration number CZ.02.2.69/0.0/0.0/18_053/0016980.
This work was supported by the Czech Technical University (CTU) grant No. SGS23/208/OHK3/3T/18.
This research was partially funded by the Engineering and Physical Sciences Research Council (EPSRC) under grants EP/R012598/1.

### Paper Origin

Part of this work was published at the MECO 2023 conference: Preucil, Tomas and Novotný, Martin. (2023). Surveying the security of access systems in Uppsala, Sweden.

# Introduction to Probing Security

David Pokorný
FIT CTU in Prague
Thakurova 9, Prague 6
david.pokorny@fit.cvut.cz

Supervisor: Dr.-Ing. Martin Novotný

Abstract

In the realm of cryptographic circuits, the preservation of secrecy, while probing their wires, is a major challenge - one addressed by the concept of probing security. This presentation delves into the principles behind probing security, demonstrating its significance in creating resilient cryptographic designs. It elaborates on standard techniques such as secret sharing, integral to constructing 'private gadgets'. The discussion progresses to the principles of Non-Interference and Strong-Non-Interference, highlighting their role in the composition of larger, secure circuits from these secured gadgets. A unique strength of probing security lies in its implication of security within the noisy-leakage model and with its potentials in automation, such as automatic proofing of security and the automatic generation of secured circuits.

Keywords— Probing Security, Side-Channel Analysis, Private Circuit

# Asynchronous IEC 61499 systems on FPGAs

Martin Resetarits
*Automation and Control Institute*
*TU Wien*
Vienna, Austria
https://orcid.org/0000-0003-4788-2664

Supervisor: *Andreas Steininger and Florian Huemer*

**Abstract**

The IEC 61499 standard facilitates the deployment of flexible decentralized control architectures. Current IEC 61499 runtime systems focus on synchronous software solutions. Only a few attempts have been made to bring the standard to FPGAs, and none investigated an asynchronous design. Although synchronous FPGA Function Blocks provide a speed-up compared to software solutions, the heterogeneous structure of complex of IEC 61499 systems may enforce multiple clock domains or an overall reduced clock frequency. This study proposes an asynchronous implementation for the event-based communication of IEC 61499. With this approach, each Function Block can work at its own maximum speed, thus increasing the overall speed. To keep the focus on the asynchronous communication, the internal function is developed as a synchronous state machine with a synchronization border between receiving events and data, and the execution of these. Furthermore, information is provided on how asynchronous state machines might be used to increase the speed of each Function Block. As a proof-of-concept, the design is built on an FPGA with randomized input variables and different clock and input frequencies.

***Keywords*— IEC 61499, Automation, FPGA, Asynchronous circuits, VHDL, Events**

## I. Introduction

Modern industry demands intelligent automation with highly adaptable components. Decentralized control structures and reconfigurable devices are key factors for a competitive and successful production line. Robust communication and well-defined interfaces enable the reuse of software, which reduces development costs.

IEC 61499 was developed to meet all demands of an architecture for highly adaptable industrial control applications. It is based on the Function Block (FB) concept of IEC 61131 and shares many of the well-defined and widely acknowledged benefits. In IEC 61499 the communication is split into data and events, whereby the latter act as control signals between FBs.

FBs are encapsulated program units and form the basic pieces of an IEC 61499 application. They react to incoming events and manipulate input data accordingly. Once the internal execution is finished, new events are created on the output side, and other FBs are triggered. IEC 61499 defines a visual representation of the interface, which can be seen in Fig. 1.

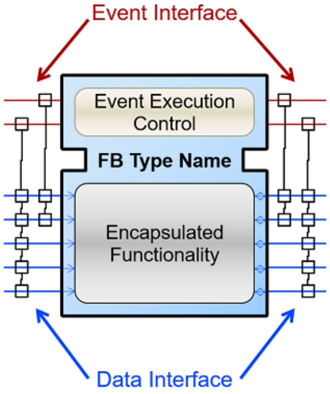


Fig. 1: Function Block Interface according to IEC-61499. Red lines are used for event wires; blue lines for data wires. Data should only be updated when a specific event arrives or is sent. This dependency is displayed as a black line with squares on the corresponding lines. Source: [1].

According to IEC 61499, all FBs operate in parallel. In Programmable Logic Controllers (PLCs) that use Central Processing Units (CPUs), only pseudoparallelism is possible, since a simple CPU can execute only one operation at a time. Therefore, the full potential can never be achieved on such architectures.

Application Specific Integrated Circuit (ASIC)s are too expensive and time-consuming in their design and fabrication for flexible industrial applications. To utilize the parallelism defined by IEC 61499 and still operate on adaptable hardware, Field Programmable Gate Arrays (FPGAs) can be used.

Despite promising benefits, only a few publications have studied the role of FPGAs for the IEC 61499 standard [2]–[4]. In [4] a bus system and a *Device Manager* are used to distribute data between several devices. In [3] the devices interact directly with each other. [2] focuses on the possibility of simultaneous events in a time-quantized environment and provides a concept to solve the resulting problems. All research investigates synchronous models for communication and FB internal execution.

This work focuses on asynchronous communication between individual FBs. First, the current state-of-the-art is reviewed, and the necessary basics of asynchronous design are given. In Section III, the concept of event-based, asynchronous communication is presented. Section IV explains the experimental system, and the results and findings are provided in Section V. Finally, Section VI provides concluding remarks.

## II. Background and state of the art

This section provides details of IEC 61499, highlighting important information on the event-based communication between FBs. Then a quick overview of synchronous IEC 61499 architectures on FPGAs is given. In Section II-C, basic concepts of asynchronous FPGA design are shown.

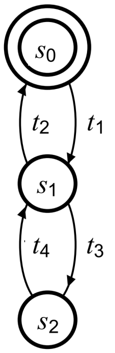
### A. *IEC 61499*

IEC 61499 defines four different types of FBs. All of them share the same interface with events and data, see Fig. 1. The Simple Function Block (SFB) has multiple algorithms of which, depending on the arriving event, one is executed. The Basic Function Block (BFB) contains a state machine defined by the user; Incoming events are used to change the state and activate associated methods.

Composite Function Blocks (CFBs) have an internal network of other FBs and are used to structure a program. It is important to note that they have an interface that has the same behavior as other FBs. This means that data is only updated when specific events arrive. Therefore, flattening a program by connecting all FBs directly and omitting the bundling CFB may change the program behavior.

Additionally, IEC 61499 defines a Service Interface Function Block (SIFB) that can be freely programmed as long as the interface specifications are met. It is used to access specific hardware, such as inports and outports.

IEC 61499 uses an event-based control flow. The procedure when an event occurs is defined with the help of a state machine, called Event Execution Control. A BFB with an internal state machine is used as an example, but the sequence is similar for all FB-types; see Fig. 2. The interface of a FB must exhibit such behavior, but the implementation of the state machine is not mandatory. FBs can only react on an event when no others are processed. In the description, it is assumed that the execution of an event is always finished when a new one occurs. When an event arrives, the data associated with this event by a *WITH* statement are updated. Then all transitions of the user-defined internal state machine are evaluated and a new state is entered if a transition is crossed. All actions linked to the new state are performed. Afterwards, transitions from this state must be checked again, as not all transitions require an event. If no transitions are crossed, the FB goes back into an idle state, waiting for new events.



| State | | Operations |
|---|---|---|
| $s_0$ | | – |
| $s_1$ | | evaluate transitions |
| $s_2$ | | perform actions |

| Transition | Condition | Operations |
|---|---|---|
| $t_1$ | an input event occurs | Sample Inputs[a] |
| $t_2$ | no transition is crossed | |
| $t_3$ | a transition is crossed | |
| $t_4$ | actions completed | |

[a] This operation consists of sampling (or its functional equivalent) of the input variables associated with the current input event by a WITH declaration

Fig. 2: The Execution Control Chart describes how arriving events should be handled for a Basic Function Block in IEC 61499.

On the output side, data are also connected to events via a *WITH* statement. This means that data are only published when an associated event is sent.

A FB can receive events and data from multiple sources; therefore, events and data are not synchronized until the FB accepts an event. Consequently, one FB might change its output value several times without any reaction from other FBs. Only when a specific event occurs, the subsequent FB samples data connections. Unused values are simply discarded.

### *B. IEC 61499 on FPGAs*

Only a few attempts have been made to bring IEC 61499 FBs to FPGAs. In [4], a FBs is divided into a BusInHandler, a FBManager, an ECCManager, an AlgoHandler, and a BusOutHandler. Each component works in a synchronous fashion. Although the standard states that such algorithms should be executed sequentially, the AlgoHandler can utilize the parallel structure of FPGAs and multiple algorithms may be scheduled simultaneously.

[3] divides the FB into three main parts; input capture, state and data management, and output emissions. The synchronous architecture uses a fall-through mechanism at the input capture stage to improve the reaction time. A speed-up of at least six orders of magnitude is reported compared to a T-CREST system [5] with the same clock frequency.

The possibility of simultaneous events in a synchronous and time-quantized environment is discussed in [2]. The proposed architecture uses a multi-write register to capture multiple events when they occur at the same time. This introduces a large overhead, although such occurrences are rare.

All of this research investigates synchronous solutions, which simplifies the design but also limits the possibilities.

### *C. Asynchronous FPGA designs*

Most hardware designs are synchronous. A single clock signal is distributed to all entities in the design. The input signals are evaluated only at the rising (or falling) edge of the clock. To guarantee correct execution, the phase skew of the clock must be minimal, which is not a trivial task. Another drawback is that the slowest instance defines the maximum frequency and therefore the execution speed of the whole design.

Asynchronous circuits are fundamentally different; instead of time quantization and clock distribution via a single signal, handshake protocols are used for synchronization. Each component acts at its own speed, forwards data when the next component is ready, and receives data when the previous one has finished its task. This behavior can be seen as fine-grained clock gating and local clocks that are not in phase [6].

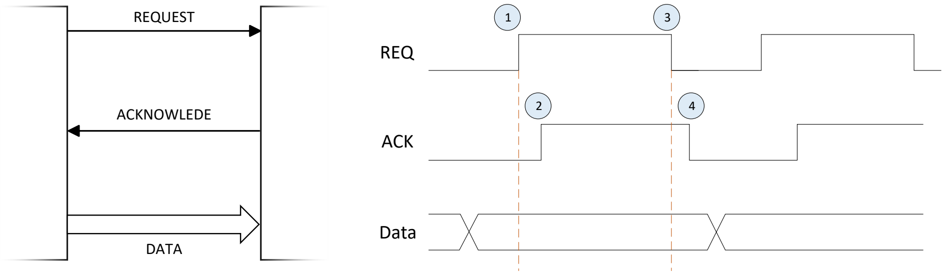
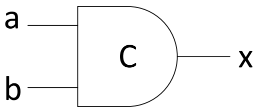


Fig. 3: 4-Phase bundled-data. On the left side the interfaces can be seen. On the right side the communication protocol. (1) First the sender issues data and sets the request signal. (2) The receiver responds with an acknowledge. (3) Now the sender can stop the request and (4) the receiver sets the acknowledge low. Then a new communication can start. The sender must guarantee stable, valid data as long as the request signal is high.

Different handshake protocols can be used to ensure data consistency in asynchronous designs. The 4-phase bundled data protocol uses a *request* and *acknowledge* pair to establish a correct data delivery. The sender states that new data are available by setting the *request* high. The receiver signals that the data was accepted by setting the *acknowledge* high. Afterwards, the sender can stop the *request* and sets the signal low. The receiver responds by setting *acknowledge* low. At this point, the sender may initiate a new request. Data must be valid as long as the *request* signal is high to guarantee correct transmission. Figure 3 shows the process.

To establish such a process, a C-Element can be used in a Muller pipeline. A C-Element is a simple module with (usually) two inports and one outport. The outport only changes when both inputs are the same; if they are different, the outport stays the same. Figure 4 shows the symbol and the truth table. On an FPGA, this behavior can be achieved by using a Look-Up Table (LUT) with the output connected as an additional input. The LUT can use this feedback wire to determine the last output in the case of two different input values.

When multiple C-Elements are combined, a Muller pipeline is formed, as shown in Fig. 5. A request is only accepted by the C-Element when the next stage sends *0* on the acknowledge wire. Then the request of this stage is forced to *1* as long



| a | b | x |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | no change |
| 1 | 0 | no change |
| 1 | 1 | 1 |

Fig. 4: Symbol and Look-Up table of a C-Element. The output only changes when both input signals have the same value.

as the next stage does not send an acknowledge and the request form the previous stage is *0*. This leads to a situation where each second request is *1*, while others are *0* when the pipeline is full.

As long as the request is *1*, the corresponding latch accepts data from the previous stage. Once the request is set to *0*, the last valid data are stored and forwarded to the next stage.

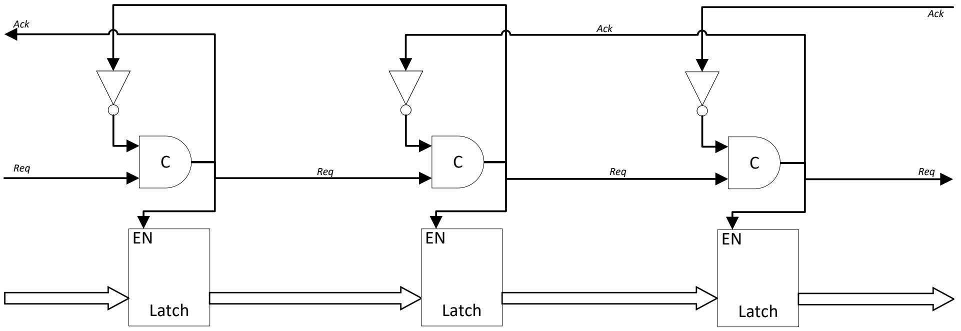


Fig. 5: Muller Pipeline

Custom logic can be added between two stages, but a well-defined delay must be introduced for the request to ensure that the data are valid before the corresponding request arrives.

An other important element for asynchronous designs is an arbiter. Its basic task is to establish a sequence between two concurrently arriving requests by first serving one and the next one afterwards. This can be used to combine two Muller pipelines into one. The important part is that only one request can be forwarded at a time. A *NAND*-based SR-latch and two additional *NAND* gates for the acknowledge feedback are used to achieve this. In the FPGA implementation, each *NAND* gate is represented by one LUT.

With Muller Pipelines and arbiters many tasks can be accomplished asynchronously. Other elements can be introduced as long as the 4-phase bundled data protocol is respected. Shortly, data must be valid as long as the request signal is high, and the request signal can only be reset when the next stage has received the data. This is signaled by the corresponding acknowledge.

## III. Concept

This work investigates an asynchronous implementation for an IEC 61499 based system. The remarkable feature of IEC 61499 is the event-based communication and therefore this part is highlighted. For the internal function of SFBs and BFBs, a synchronous design is used. Thus, clock synchronization is required once an event is accepted. As data and events are independent until synchronization, a natural separation of sub-modules occurs. These sub-modules are the event input, event output, data input, and data output module. Additionally, the internal synchronous function forms one more module. Only the latter cannot be described in a generic way, as it involves the user-defined program. An overview of the concept can be seen in Fig. 6.

The event input module needs an arbiter, as multiple events can arrive simultaneously. The synchronous logic is too slow to process multiple events when they arrive in one clock cycle. Therefore, a Muller pipeline is used as an additional buffer. It is assumed that the pipeline always has enough free space to accept an incoming event. Similar assumptions were made in all other publications for FPGAs and General Purpose Processors (GPPs), and, in essence, by not considering any back pressure, even the IEC-61499 standard suggests this. Therefore, no back pressure functionality is implemented in this work either. The concept of implementation can be seen in Fig. 7.

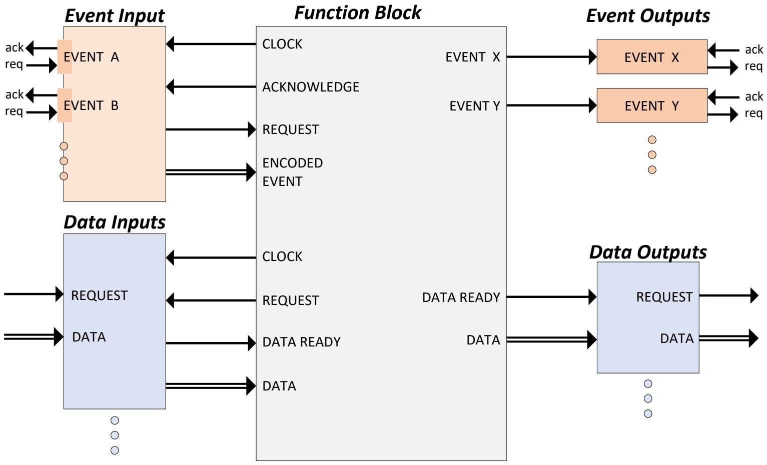


Fig. 6: Overview of the concept. On the upper left side, the event input can be seen. Each event consists of a request input and an acknowledge output. On the bottom left, one data input is sketched. Each data input needs one block. In the middle, the synchronous Function Block is shown. The clock signals to the previous modules are needed for synchronization. The event outputs are shown on the top right side. As these outputs are independent from each other, each output is implemented with one module. One example data output can be seen at the bottom right. Again each data output uses its own module.

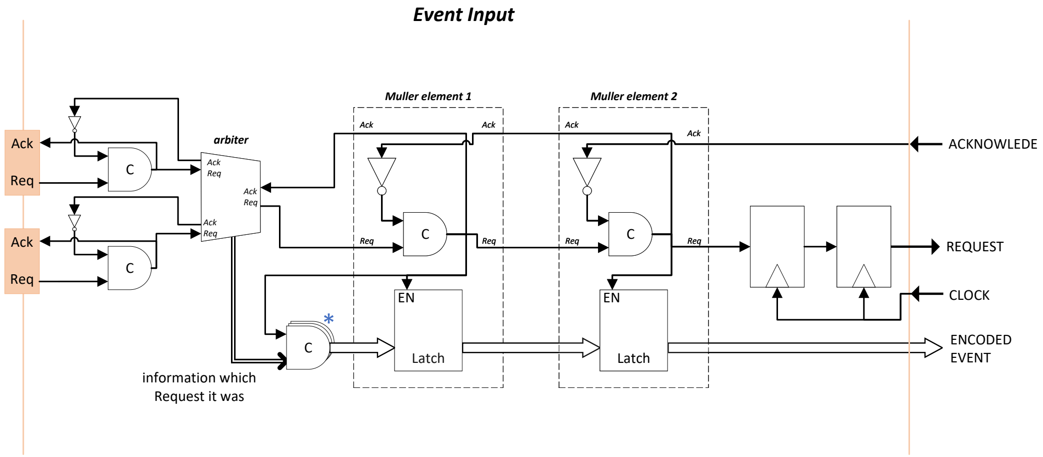
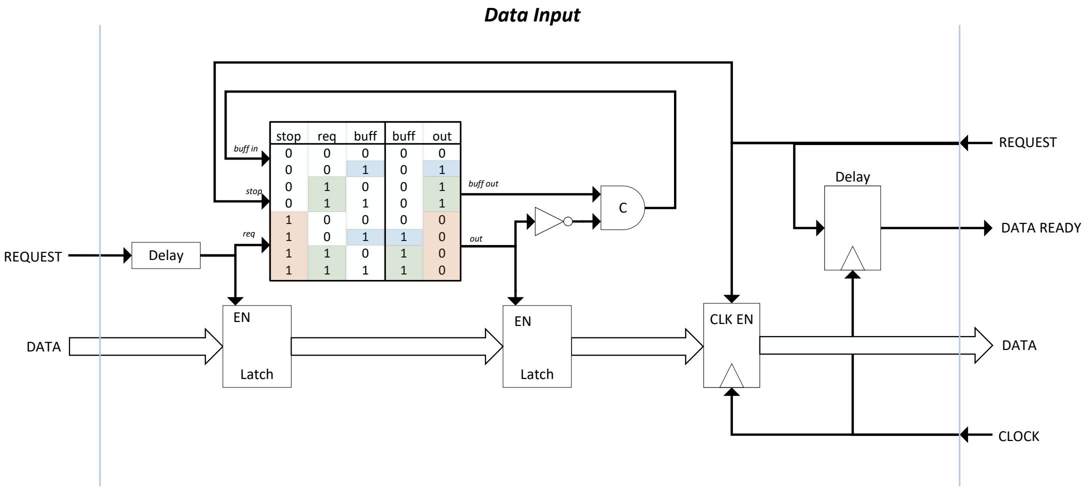


Fig. 7: The event input module. An arbiter is needed, as multiple events may occur at the same time. If more than two events are present, an arbiter cascade can be used. Each arbiter provides information about which input triggered the outgoing request. As this information is reset faster than the outgoing request, and thus the enable signal for the latch, the C-Elements marked with a blue star are necessary. They ensure that the information is valid as long as the enable signal for the latch is high. The figure shows two Muller elements, but the amount just determines the buffer depth but does not change the functionality of the concept. In the end, two synchronization flip-flops are used to ensure a stable signal for the synchronous part of the design.

Figure 8 shows the data input module. Only the newest data are of interest, and unused data are discarded. During a readout, the data must be stable, but according to IEC 61499 data can change at any time. Therefore, a two-stage buffer is required. The first stage is always ready to save new data when they arrive, overriding old data. The second stage keeps the data stable during a readout. Only when the readout is finished, new data from the first stage are loaded into the second stage.

In the event output, it is important that the request signal is only high as long as no acknowledge was received. The synchronous signal from the Function Block must be de-synchronized. In order to do so, a small state machine is used, which can be seen in Fig. 9. The Function Block can set a request, but it is reset by the acknowledge signal, regardless of the logical value sent by the Function Block output. The Function Block must send *0* between two event requests. Again, it is assumed



| stop | req | buff | buff | out |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 |

Fig. 8: The data input module. The left *request* signals that new data are available. The Look-Up table forwards the request until the *stop* signal is high. This *stop* is issued when the Function Block wants to read its input data. In this case, the second latch holds the last captured data. When new data is published by the previous Function Block, the request gets delayed. The inverter and the C-Element are used to buffer it until *out* is high again and the newest data gets forwarded. The synchronization flip-flop is only active when the Function Block wants to read its input. As this introduces a delay of one clock cycle, a second flip-flop is used for the *data ready* signal.

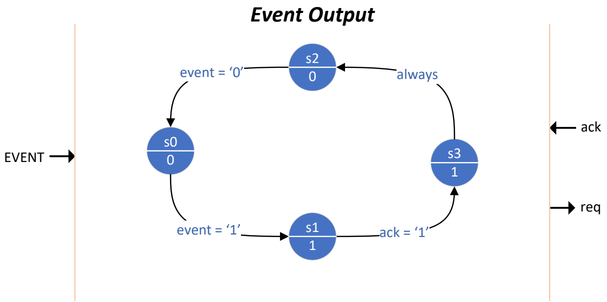


Fig. 9: The event output module. A state machine to hold every *req* until the corresponding *ack* was received. The Gray encoding of the states ensures that no unwanted transition happens due to wire delays.

that the asynchronous functions are much faster than the synchronous part. Therefore, the state machine reaches the state *0* before the Function Block sends a new request.

The data output module simply forwards the data and sends a request whenever new data are available. The Function Block changes the output data only every second clock cycle. This ensures that the *data ready* signal, which is used as *req*, is *0* between data publishing instances.

## IV. Experiment Setup

The generically described parts are tested in an Add/Sub-FB. Three of these FBs are connected to form a small network that is used to study the behavior on an FPGA.

The Add/Sub-FB can be seen in Fig. 10. It has two data inputs and two event inputs, whereby the events are used to trigger either an addition or a subtraction. Both data inputs are associated with both events; thus, the current value is sampled before the operation starts. To investigate the general case, a BFB is used to describe the internal function. The state machine can be seen in Fig. 10. It consists of 3 states, whereby one state is the idle state, and the other two are used to calculate the output.

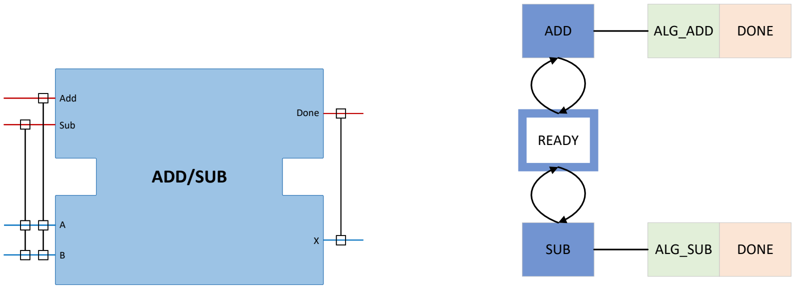
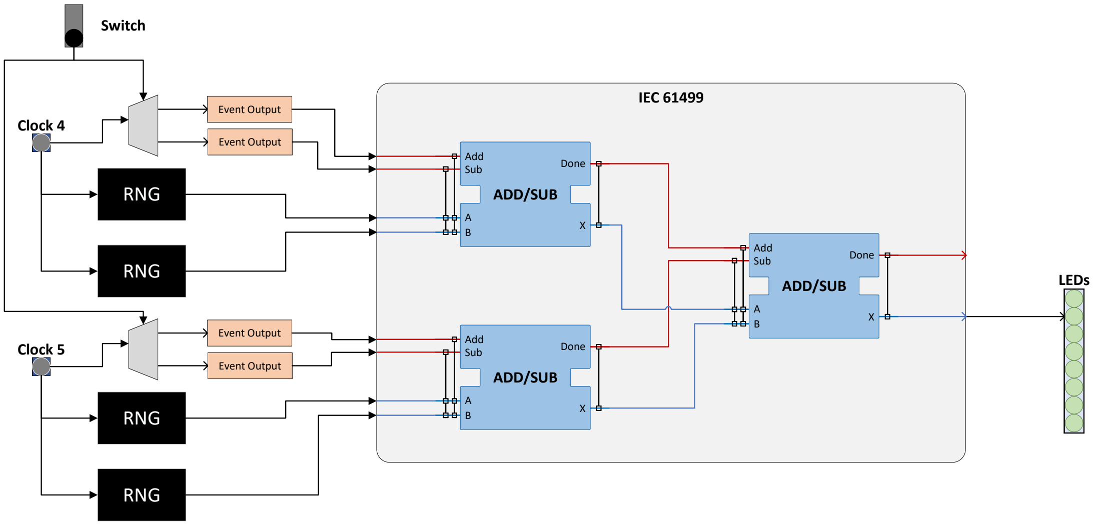


Fig. 10: Add/Sub-Function Block. On the left side the interface with event and data in-/outports can be seen. On the right, the internal state machine is shown. When a state is entered the associated algorithm (green) is executed and once finished the event (red) is fired.

Figure 11 shows the program network. Each FB has its own clock with a different frequency. The input data are generated by a random number generator, whereby two additional, much slower clocks are used to change the values. This slow clock also generates the events to execute an addition or subtraction of the first two Add/Sub-FBs. The onboard switches are used to change the operation. Only the three FBs are designed according to IEC 61499, other modules are used as testbench and do not follow any industrial standard.



| Name | Frequency [MHz] | Name | Frequency [MHz] |
|---|---|---|---|
| FB1 | 56 | Clock 4 | 1 |
| FB2 | 75 | Clock 5 | 0, 6 |
| FB3 | 100 | | |

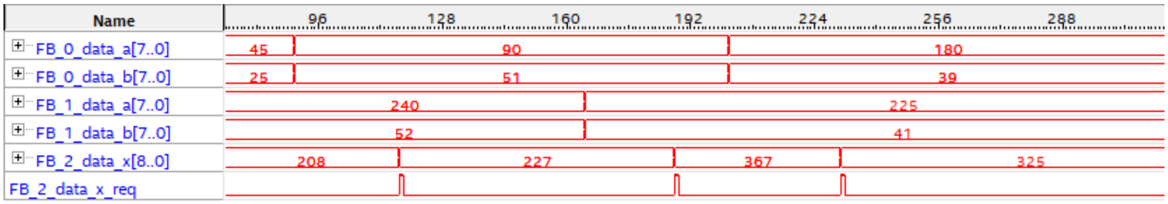
Fig. 11: Test Network and clock frequencies. Inside the gray box, communication is based on the asynchronous 4-phase bundled data protocol. Modules outside the gray box are part of the testbench and do not follow the IEC 61499.

## V. Results

### A. Execution speed

The test bench and the network were synthesized with the Intel©Quartus©Prime software and downloaded to a Cyclone IV E FPGA. To demonstrate the feasibility of the proposed concept, the Quartus©Signal Tap Logic Analyzer (STLA) is used. The input and output data is probed to ensure correct behavior of the network. As sampling frequency 112 MHz was chosen.

Figure 12 shows the waveform of the STLA. The system works as intended and computes correct results. It can be observed that the timing between the input and the output is not regular. This is due to the fact that each FB has its own frequency and therefore the time between sending and accepting new events fluctuates.



| input cycle | calculation | result | output cycle |
|---|---|---|---|
| $\leq 89$ | $(45 - 25) + (240 - 52)$ | $= 208$ | $\leq 116$ |
| 90 | $(90 - 51) + (240 - 52)$ | $= 227$ | 117 |
| 165 | $(90 - 51) - (225 - 41)$ | $= -145 \equiv 367$ | 188 |
| 202 | $(180 - 39) + (225 - 41)$ | $= 325$ | 231 |

Fig. 12: Signal tap logic analyzer wave form. The table below shows the calculation and the timing of each signal. In the third line an underflow happens.

Comparing the reaction time, which is between 200 ns and 250 ns, the system is slower than synchronous applications. A closer inspection revealed that the synchronization of the event input and the data input creates the highest delay.

### B. Increasing the execution speed

To eliminate this delay, an asynchronous state machine can be used for the internal function. The interface between the Function Block and the Event Input module already has a request and acknowledge signal. For the event outputs and the data outputs, the acknowledge from the next FB can be forwarded. In the case of the Data Input module, small changes must be made, but the general concept remains the same. From the outside, this module looks like a sink that can always accept new data. With the request signal from the Function Block, the newest data is forwarded. To ensure that this data is stable, the second latch must be disabled during readout. The flip-flop must be replaced with a latch that is enabled by the inverted enable signal of the second latch. By combining this signal and the request signal with a logical *AND*, the acknowledge signal can be formed. This ensures that the data is valid and stable as long as the request signal is high.

In addition, many FBs are rather simple, but are often used. As an example, a rendezvous FB waits until two specific events have occurred and then fires a new one. Creating custom, asynchronous solutions for specific tasks like this without the use of the generic template is trivial but will increase the execution speed drastically, and these can be reused in each new project.

## VI. Conclusion

The decentralized programming paradigm of IEC 61499 is an interesting target for science and industry. The function is divided into multiple parallel running subunits, called Function Blocks (FBs). Although FPGAs seem to be a perfect fit for such a system, only a few researchers showed interest in this topic. All of them investigate synchronous solutions and report an increased performance.

This work presented an asynchronous concept for the event-based communication described by IEC 61499. To simplify the analysis, the internal function of each BFB was executed synchronously. The feasibility of the concept was proven by tests conducted on a Cyclone IV E FPGA. For these tests, multiple FBs were connected to form a network and random generated input values were used. However, performance was lower than in synchronous implementations.

Consequently the possibility of using asynchronous state machines was discussed. This improvement is simple to integrate and eliminates the biggest drawback of the proposed solution; the delay introduced by the synchronization.

## References

[1] Eclipse. 4diac - Framework for Industrial Automation & Control. [Online]. Available: https://eclipse.org/4diac/

[2] M. Resetarits, M. M. Merkumians, and G. Schitter, "Controlling concurrent events in iec 61499 based systems on fpgas," in *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2022, pp. 1–4.

[3] H. Pearce and P. Roop, "Synthesizing IEC 61499 function blocks to hardware," in *2019 International Conference on Electronics, Information, and Communication (ICEIC)*. IEEE, jan 2019.

[4] D. O'Sullivan and D. Heffernan, "VHDL architecture for IEC 61499 function blocks," *IET Computers & Digital Techniques*, vol. 4, no. 6, pp. 515–524, nov 2010.

[5] H. Pearce, P. Roop, M. Biglari-Abhari, and M. Schoeberl, "Faster function blocks for precision timed industrial automation," in *2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)*, 2018, pp. 67–74.

[6] J. Sparsø, *Introduction to Asynchronous Circuit Design.* DTU Compute, Technical University of Denmark, 2020, paperback edition available here: https://www.amazon.com/dp/B08BF2PFLN.

# Processing and Analysis of Accelerometer Data for the Surface State Identification

Yegor Boyarchikov
*Institute of Mechatronics and Computer Engineering (MTI)*
*Technical University of Liberec*
Liberec, Czech Republic
egor.boyarchikov@gmial.com

Supervisor: *Tomáš Martinec*

## Abstract

Abstract—Data collecting, analysis, and processing play a big and very important role in spheres that are connected with the following areas: transport, medicine, industry, etc. The author proposes to analyze existing methods and approaches of data analysis, collecting, and processing. Based on this overview, it is supposed to develop new solutions for the probable implementation in the following areas: design of the autonomous mobile platforms. In order to increase the performance and decrease response time, it is planned to test the probability of using such solutions as edge computing. According to the results of the research, it is planned to choose the most optimal algorithms and approaches, based on it develop own solutions for further probable implementation in spheres like autonomous transport systems, smart systems, industry 4.0, medicine, etc.

***Keywords— Z-THRESH, Z-DIFF, G-ZERO, accelerometer, road defect identification, autonomous mobile platform, accelerometer signal analysis, road pavement defects detection, machine learning, accelerometer data processing, accelerometer***

## I. Introduction

Objective of surface state monitoring requires many attention and resources. For such purpose we may use static sensors, but installation of large sensors network is very expensive solution. If we speak about relativelly big areas of the surface, application of the static methods for the road state analysis also seems unsuitable. For example, rod and level mehod is one of the well known methods for the static road state analysis [1]. The huge size of the road network makes application of static methods challenging in terms of cost and labor. This task can be solved by adding inexpensive and easy-to-install data collection equipment, which will simplify the process of road quality monitoring.

Researchers already were trying to solve these problems. Vehicle Intelligent Monitoring System (VIMS) was developed. An accelerometer, a microscope, a GPS and laptop are installed in an ordinary road patrol car, but this system has advantages and disadvantages [2]. VIMS was designed at the beginning of the century. This work is intended to use previous experience and improve it with present approaches. As it was mentioned before surface state monitoring is complex and complicated task. Even 20 years ago it was impossible to imagine existence of mobile measuring units for such purposes.

Nowadays miniaturization in combination with growth of mass production allow researchers to design measuring units and platforms equipped with sensors such as digital accelerometers, cameras, LiDARs and gyroscopes. For example, there are already many projects in the field of road pavement monitoring; there are many different approaches such as 3D data analysis [4], vibration data analysis [5], and image analysis [6].

This work contains the description an overview of the several methodics used for the purpose of the road pavement state classification from such simple as Z-Thresh to the application of several architectures of the Neural Networks.

## II. Methods and Aproaches

Z-THRESH – the first and the simplest algorithm, which could be used for the road defects identification. This approach is based on the axis data processing. Function for the axis data classification is a border function that contains the desired value fig.1. Based on this value algorithm performs classification of the road defect. For example, it is possible to identify dump, crack or sequence of the defects

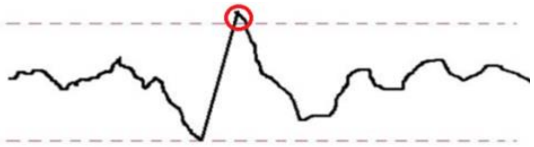


Fig. 1. Z-THRESH algorithm for road defect identification.

Z-DIFF – a more advanced type of algorithms for road defects identification. This method is also based on axis data processing. The classification function of the Z-DIFF algorithm is a border filter. This function performs a classification of the difference between two subsequent values fig. 2. This approach allows for identifying fast changes in acceleration on a vertical axis. Based on this it is possible to identify the type of the defect and classify the type of the surface.

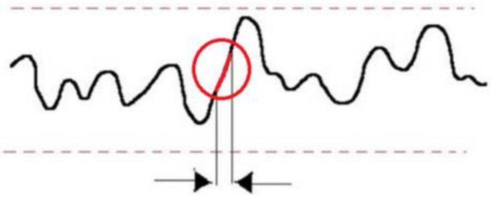


Fig. 2. Z-DIFF algorithm for road defect identification.

G-ZERO is an algorithm for surface defect identification. While using visual data analysis tools and searching for specific data patterns researchers found that there exist certain events characterized by measurement tuple. During the experiments, it was discovered that in a moment of passing dump or crack values of the accelerometer demonstrate definite dynamics. The empirical analysis of the data had led to the following conclusions: 1) such data tuples could be acquired when the vehicle was in a temporary free fall, for example, entering or exiting a pothole; 2) such data tuples could be analyzed without information about exact Z-axis position of the accelerometer. The researchers named this algorithm G-ZERO fig. 3 after the main feature of the detected event.

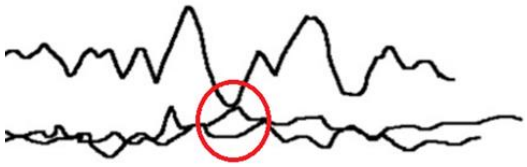


Fig. 3. G-ZERO algorithm for road defect identification.

As was said before another idea of the data processing in the field of road pavement state monitoring is an application of the Neural Networks. In our case, we used Long Short-Term Memory Recurrent Neural Networks (LSTM) and their modifications: CNN-LSTM and ConvLSTM. LSTM network models are a type of Recurrent Neural Network that can effectively learn and retain information over long sequences of input data, making them suitable for data consisting of hundreds of steps.

Several results of the application of the mentioned Neural Networks are shown below fig. 4. Blue curve – original signal from the accelerometer. Red curve – the identified defects. Green windows show the differences in identification for different Neural Networks.

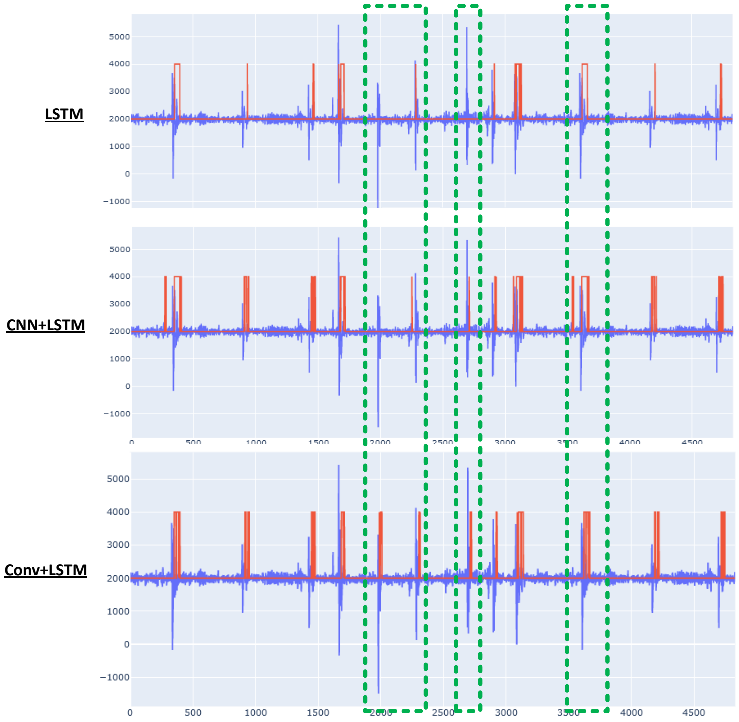


Fig. 4. Comparison of the LSTM and modifications

From the first sight such simple methods as Z-THRESH or Z-DIFF look more attractive for the pavement defects identification or binary classification of the pavement (defect or not defect) because of the relative simplicity. However, LSTM and modifications also show good performance in this domain. According to the nature of the task, we chose the following metrics to assess the performance:

- recall - the metric, that indicates that the desired defect of the pavement occurs;
- precision - the metric, that is the proportion of correct positive combinations among all combinations.

TABLE I METRICS SUMMARY

| Model | Precision | Recall |
|---|---|---|
| LSTM | 0.79 | 0.65 |
| CNN-LSTM | 0.67 | 0.73 |
| ConvLSTM | 0.80 | 0.78 |

As could be seen from the values in Table I, CNN-LSTM and ConvLSTM compared to the basic LSTM, have an 8-11% larger recall value, at the same time, comparing of the CNN-LSTM and ConvLSTM, shows that, the ConvLSTM has up to a 13% increase in the precision metric.

Why Neural Networks were chosen as possible tool for the task? LSTM and modifications are supposed to be used in more extended meaning. We plan to expand amount of the defect classes. The application of the Neural Networks such as LSTM, CNN-LSTM or ConvLSTM will provide us this opportunity.

## ACKNOWLEDGMENT

Special acknowledgment to my supervisor Ing. Tomáš Martinec Ph. D.

## PAPER ORIGIN

The materials for this abstract were taken from the author’s papers in the ICCC 2020 and ICECCME 2023.

## REFERENCES

[1] M. Sayers, S. Karamihas, The Little Book of Profiling: Basic Information about Measuring and Interpreting Road Profiles, University of Michigan. Transportation Research Institute, UMTRI, 1996.

[2] T. Furukawa, “VIMS Manual,” Japan, VIMS Consortium, Nagasaki University, 2012.

[3] B. Lanjewar, J. Khedkar, R. Sagar, R. Pawar, K. Gosavi, “Survey of road bump and intensity detection algorithms using smartphone sensors,” IJCSIT, Vol. 6, 2015

[4] Shen-en & Liu, Wanqiu & Bian, Haitao & Smith, Ben. (2012). 3D LiDAR scans for bridge damage evaluation. Forensic Engineering 2012: Gateway to a Better Tomorrow - Proceedings of the 6th Congress on Forensic Engineering, pp.487-495, doi: 10.1061/9780784412640.052.

[5] Fergyanto Gunawan. Detecting road damages by using gyroscope sensor. ICIC Express Letters, 12:1089– 1098, 11 2018, doi: 10.24507/icicel.12.11.1089.

[6] Andres Angulo, Juan Antonio Vega-Fern´andez, Lina Maria Aguilar-Lobo, Shailendra Natraj, and Gilberto Ochoa-Ruiz. Road damage detection acquisition system based on deep neural networks for physical asset management. In Lourdes Mart´inez-Villase˜nor, Ildar Batyrshin, and Antonio Mar´in-Hern´andez, editors, Advances in Soft Computing, pp. 3–14. Springer International Publishing, 2019.

# Artificial intelligence enabled preliminary diagnosis for COVID-19

Carmi Shimon
Afeka Tel Aviv Academic College of Engineeringail
Mivtsa Kadesh St 38, Tel Aviv-Yafo, 6910717 Israel
carmis@mail.afeka.ac.il

Inbal Dangoor
Afeka Tel Aviv Academic College of Engineering
Mivtsa Kadesh St 38, Tel Aviv-Yafo, 6910717 Israel
Dangoor.Inbal@mail.afeka.ac.il

Supervisor: *Gabi Shafat, Afeka Tel Aviv Academic College of Engineering. gabis@ afeka.ac.il*

## Abstract

The COVID-19 outbreak was announced as a global pandemic by the World Health Organization in March 2020 and has affected a growing number of people in the past few months. In this context, advanced artificial intelligence techniques are brought to the forefront as a response to the ongoing fight toward reducing the impact of this global health crisis. In this study, potential use-cases of intelligent speech analysis for COVID-19 identification are being developed. By analyzing speech recordings from COVID-19 positive and negative patients, we constructed audio - and symptomatic-based models to automatically categorize the health state of patients, whether they are COVID-19 positive or not. For this purpose, many acoustic features were established, and various machine learning algorithms are being utilized. Experiments show that an average accuracy of 80% was obtained estimating COVID-19 positive or negative, derived from multiple cough and vowel /a/ recordings, and an average accuracy of 83% was obtained estimating COVID-19 positive or negative patients by evaluating six symptomatic questions. We hope that this study can foster an extremely fast, low-cost, and convenient way to automatically detect the COVID-19 disease.

## I. Introduction

Scientists and researchers from a bench of research domains are stepping up in response to the challenges raised by the COVID-19 pandemic and its consequences. Meanwhile, methods and technologies have been designed and investigated to accelerate diagnostic testing speed [1].

A lot of data driven efforts have been made regarding to the Covid-19 pandemic. In particular, a number of works have proposed the promotion of sound-based COVID-19 assessment. For instance, in [1], a model based on a convolutional neural network (CNN) was developed to extract visual features from mel-spectrogram images to classify four cough types (COVID-19, pertussis, bronchitis, and normal).

From the perspective of sound analysis, as coronavirus is a respiratory illness, abnormal breathing patterns from patients intuitively might be a potential indicator for diagnosis of sleep quality, anxiety, fatigue [2], or any other abnormal respiratory activity [3]. Other research explores the changes in the acoustic parameters of voice in COVID-19 patients [4]. Various typical respiratory symptoms can be observed, from dry cough presented in mild illness to shortness of breath in moderate illness and, further, severe dyspnea, respiratory distress, or tachypnea in severe illness [5].

In this research, we investigate the importance of analyzing voice or speech signals and a short questionnaire regarding this virus pandemic in an empirical manner. As part of an early study on the intelligent analysis of voice cues under COVID-19, a data-driven approach automatically detects the patients' health status.

## II. DATA COLLECTION

Since the COVID-19 pandemic is still spreading, data collection and annotation is an ongoing task. At present, data collection is under way worldwide from both infected patients at various stages of the disease and healthy individuals as a control group. Researchers from Vocalis-Health Company, the Afeka Center for Language Processing (ACLP), and Matrix IT Ltd., have launched a new app to gather voice samples as well as a short query regarding symptoms such as fever, shortness of breath, tiredness, etc. Researchers from Carnegie Mellon University (CMU) have launched a new web page3 as a “COVID-19 Voice Detector” to gather voice samples, such as coughs, several vowel sounds, counting up to 20, the alphabet, etc. Nonetheless, currently all these data are not publicly available for research purposes according to the Helsinki Committee. The recordings from CMU are self-recorded, i.e., no medical doctor has confirmed the patient's status. As for the Israeli Defence Forces (IDF) data collection, the process took place in Israel using the Vocalis-Health app. Medical doctors who instructed verified COVID-19 positive and negative patients on how to record themselves supervised it. At this point, data collection between March 6 and June 13, 2020, is being used and processed. While doctors were making their daily rounds to check the patients at the hospitals, they recorded each patient individually. Data collection from IDF consists of three vowels (/a/, /s/, and /z/), coughs, a short reading passage, and counting from 50 to 80 in the Hebrew language. The focus is on cough and /a/ vowel recordings solely based on experimental results. Furthermore, regarding demographic information from both datasets, two characteristics of the patients were collected: age and gender.

As of June 13, 2020, the text data collection contains 173 questionnaires from 57 patients, 25 of them COVID-19 positive and 32 negative. Forasmuch as patients stayed at the hospital for more than 1 day, some of them answered the questionnaire multiple times, in particular, 1–16 times. The following six questions were asked in the questionnaire: (1) How bad is your shortness of breath today? (2) How bad is your cough today? (3) How bad is your snot today? (4) Have you measured fever over 37.8 °C today? (5) Is there a change in the sense of smell? (6) In relation to the earlier days, how do you feel today?

Audio quality: The voice capturing process from CMU was done using an application installed in the patient's smartphone, which applied post processing to the audio signal and used compression by various vocoders. While for most of the people, this fact will make no difference; this process makes changes in the RAW audio file.

## III. DATA COLLECTION

A series of data preprocessing processes were implemented, specifically the following three processes.

### *A. Data cleansing*

Recordings were made in hospitals, in a noisy environment. Consequently, recordings that contained both noisy background and shorter than 500ms for vowel /a/, and shorter than 100ms for coughs were discarded, since some patients were experiencing difficulties pronouncing.

Regarding vowels /a/, 5% of leading and trailing samples were trimmed out to avoid inhale or exhale effects.

### *B. Voice activity detection*

AUDACITY software was used to segment coughs for each voiced segment in case a recording consisted of multiple coughs in a row. Following audio-data preprocessing, a total number of 1296 segments for coughs and 428 segments for /a/ vowels existed for audio experiments. In total, 1728 audio segments were collected with a sampling rate of 44 kHz for further analysis.

### *C. Text data quantization*

Since the answers for the questionnaire were in words (none, very mild, discomforting, moderate, severe, and very severe), a quantization had to be done, i.e., answers were converted to numbers between 1 and 6 and then normalized using min-max normalization to numbers between 0 and 1.

## IV. FEATURE EXTRACTION

Three acoustic feature sets are considered in this study. First was the Computational Paralinguistics Challenge (ComPARE); specifically, these feature sets were extracted with the openSMILE toolkit [6]. Second was a combination of acoustic features extracted from a freely available script and libraries with the open-source software, praat and librosa. The first is a software that analyses, synthesizes, and manipulates speech.4 The second is a python library for audio and music analysis [7]. Another acoustic feature-set is a 1024 embedding feature vector, extracted per utterance using a deep convolutional neural network (D-CNN). The D-CNN model was prior trained for weakly labeled audio by [8] using the ESC-50 dataset.

The ComPARE feature set is a large-scale brute-force set [9]. It contains 6373 static features by computing various statistical functionals over 65 low-level descriptor (LLD) contours, cepstral, prosodic, and voice quality features. For more details, the reader is referred to [9].

Similar to the large-scale ComPARE set, a smaller feature set is based on praat4 and librosa [7]. It contains 65 static features by computing various statistical functionals over some other LLD. 65 features are carefully selected based on trial and error on COVID-19 positive and negative recordings, using RF tests.

Another feature set applied in this work is based on a D-CNN model [8], which was designed and trained to classify 2000 weakly labeled environmental audio recordings from the ESC-50 dataset. Then [8] used transfer learning on 50 different classes of speech and environmental sounds where one of them was coughs. The last layers of the D-CNN were the 1024 embedding feature vector and a classification layer. For more details, the reader is referred to [8]. The researchers' aim is COVID-19 identification. An audio recording (cough or /a/) is the input of the neural network, while the output is a 1024 embedding feature vector from the D-CNN model to be used as a feature set.

In addition to the audio recordings, a six value vector, quantized between 0 and 1 was used according to the questionnaire answers from the IDF data collection.

## V. EXPERIMENTS

In this work, the evaluation of the three feature sets is against two classifiers: a support vector machine (SVM) with a radial basis function (RBF) and a random forest (RF). SVMs are known as both linear and non-linear classifiers that map input features into high-dimensional feature spaces, allowing them to find the best separation between classes. RFs are an ensemble learning method for classification and operate by constructing a multitude of decision trees at training time and outputting the class that is the mode of the classes. They both work well for small and large amounts of data, differing from neural networks, which require a large amount of data for training. The two classifiers were implemented in python using the scikit-learn library. Many parameters were tuned to get the best results, specifically, for the RF classifier, 20 estimators (number of trees) with a maximum

depth of 4 for each tree. As for the SVM classifier, considering linear, polynomial, and RBF kernel functions, the most separating kernel was found to be the RBF one. Furthermore, to deal with the imbalanced data during training, a class weighting strategy was employed.
For all experiments in this study, the same train-set and test-set were used.

## VI. RESULTS

Handcrafted features, which were extracted using praat and librosa, performed better than the 1024 embedding feature vector and ComPARE feature set, in both RF and SVM classifiers, achieving 0.76 accuracy.

The 1024 embedding feature vector, which extracted using D-CNN for sound events and scenes [8], performed much better than the other feature sets. Note that the RF classifier performed better than the SVM classifier, achieving 0.73 accuracy, 0.69 AUC, and 0.81 F1-score. The best performance was taken where the highest AUC was obtained, and performance in terms of accuracy

## VII. DISCUSSION

In this preliminary study, experiments were carried out based on speech recordings and a self-reported questionnaire, from COVID-19 infected and hospitalised patients. The results have demonstrated the feasibility and effectiveness of audio-and-text-based COVID-19 analysis, specifically in predicting the health status of patients. Nonetheless, there are still many ways to extend the present study for further development. First, the collected dataset is relatively small and lacks patients with other respiratory diseases. Hence, further research must be established to investigate whether the classifier can distinguish between other respiratory diseases and COVID-19. Additionally, we do not know the medical background of the patients, which may bias the classification task. Therefore, the COVID-19 positive and negative terminology is used.

These data collections are still in progress for more comprehensive analysis in the future. Also, given more data, the performance of our models is expected to be further improved and more robust. Moreover, in addition to conventional handcrafted features, deep representation learning algorithms might be explored to learn representative and salient data-driven features for COVID-19 related tasks. In this study, the classification results based on days recording during hospitalisation are much better than the results per-patient (all day recordings), as can be seen in Table IV. We assume these findings are related to the fact that COVID-19 positive individuals are recovering over time; therefore, their respiratory symptoms become less apparent.

## ACKNOWLEDGMENT

We would like to thank all researchers, health supporters, and anyone else these days helping to fight against COVID-19. This work is dedicated to those affected by the virus. We thank the IDF and the Afeka College of Engineering for their support and express special gratitude to Professor Mirian Furst-Yust for her guiding lines. The authors also thank Eli Friedman, Shmuel Makmal, Ido Meister, Shay Perlmutter, and Elron Goldemberg from the DDRD who led the data collection and the multidisciplinary, multi-center, national research project.

## PAPER ORIGIN

**The Original Source of this paper: The Journal of the Acoustical Society of America-JASA, Volume 149, Issue 2, February 2021.**

## REFERENCES

[1] Durner, J., Burggraf, S., Czibere, L., Fleige, T., Madejska, A., Watts, D. C., Krieg-Schneider, F., and Becker, M. (2020). "Fast and simple highthroughput testing of COVID 19," Dent. Mater. 36, e141–e142.

[2] Han, K., Qian, M., Song, Z., Yang, Z., Ren, S., Liu, J., Liu, H., Zheng, W., Ji, T., Koike, X., Li, Z., Zhang, Y., Yamamoto, Y., and Schuller, B. W. (2020). "An early study on intelligent analysis of speech under COVID-19: Severity, sleep quality, fatigue, and anxiety,"

[3] Wang, Y., Hu, M., Li, Q., Zhang, X.-P., Zhai, G., and Yao, N. (2020). "Abnormal respiratory patterns classifier may contribute to large-scale screening of people infected with COVID-19 in an accurate and unobtrusivemanner," arXiv:2002.05534.

[4] Asiaee, M., Vahedian-azimi, A., Shahab Atashi, S., Keramatfar, A., and Nourbakhsh, M. (2020). "Voice quality evaluation in patients with COVID-19: An acoustic analysis," J. Voice (published online).https://doi.org/10.1016/j.jvoice.2020.09.024.

[5] Cascella, M., Rajnik, M., Cuomo, A., Dulebohn, S. C., and Di Napoli, R. (2020). "Features, evaluation and treatment coronavirus," in Statpearls [Internet] (StatPearls Publishing, Treasure Island, FL).

[6] Eyben, F., Wöllmer, M., and Schuller, B. (2010). "Opensmile: The Munich versatile and fast open-source audio feature extractor," in Proceedings of the 18th ACM International Conference on Multimedia, pp. 1459–1462.

[7] McFee, B., Raffel, C., Liang, D., Ellis, D. P., McVicar, M., Battenberg, E., and Nieto, O. (2015). "librosa: Audio and music signal analysis in python," in Proceedings of the 14th Python in Science Conference, Vol. 8, pp. 18–25.

[8] Kumar, A., Khadkevich, M., and Fügen, C. (2018). "Knowledge transfer from weakly labeled audio using convolutional neural network for sound events and scenes," in Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), April 15–20, Calgary, Canada, pp. 326–330.

[9] Schuller, B., Steidl, S., Batliner, A., Vinciarelli, A., Scherer, K., Ringeval, F., Chetouani, M., Weninger, F., Eyben, F., Marchi, E., Mortillaro, M., Salamin, H., Polychroniou, A., Valente, F., and Kim, S. (2013). "The INTERSPEECH 2013 Computational Paralinguistics Challenge: Social signals, conflict, emotion, autism," in Proceedings of INTERSPEECH 2013, 14th Annual Conference of the International Speech Communication Association, Lyon, France.

# Optical Fault Injection Attacks against Different Logic and Memory Cells

Dmytro Petryk[1] and Zoya Dyka[1,2]
[1]*IHP – Leibniz-Institut für innovative Mikroelektronik, Frankfurt (Oder), Germany*
[2]*BTU Cottbus-Senftenberg, Cottbus, Germany*
{petryk, dyka}@ihp-microelectronics.com

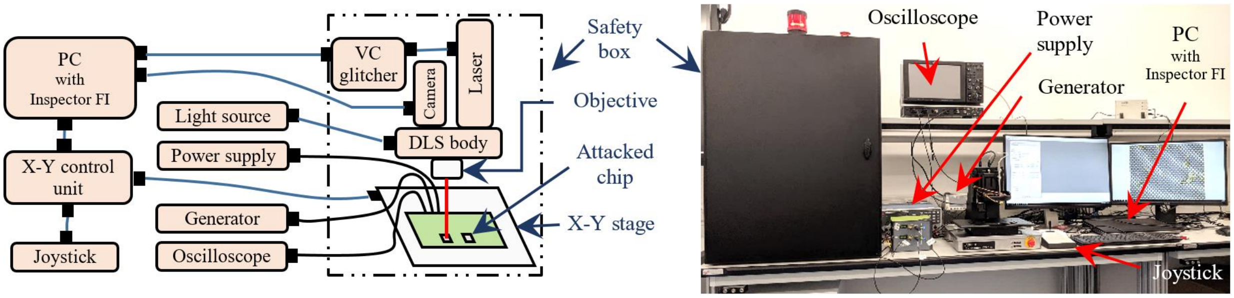
Semiconductor devices are widely used for industrial control systems, smart cities, battery powered devices for e-health, the Internet of Things, etc. Plenty of the devices are developed to operate with private data, i.e. the data processed and stored in them have to be protected from the malicious users. The crucial security requirements for such devices are confidentiality, data integrity, authentication, services availability, authenticity and non-repudiation. To guarantee them cryptographic algorithms are used, where the secrecy is based on the secrecy of the private/secret keys. From mathematical point of view these algorithms using keys with recommended lengths are secure. The issue is that usually physical access the devices can be gained, i.e. a potential attacker can steal and attack them in a specialized lab. Practically, many physical attacks are aimed to extract cryptographic keys or cause data leakage and are much more effective than brute force.

Some physical attacks exploit the fact that different cryptographic operations performed consume different power and also depend on the cryptographic key processed. To realize the attack an attacker can measures the so-called side-channel effects during a cryptographic operation, e.g. current drawn from the power supply, electromagnetic radiation, execution time, etc. The measured data can be then analysed using statistical, machine learning or artificial intelligence methods with the goal to reveal the key. Such attacks are known as Side-Channel Analysis (SCA) attacks. Other class of physical attacks are different manipulations exploiting the sensitivity of semiconductor devices to their environmental and working parameters: temperature, operating voltage, frequency, electromagnetic pulses, light, and so on. The goal of an attacker is to inject the faults that cause incorrect output of cryptographic operations. The used cryptographic key can be revealed analysing the incorrect outputs. These attacks are known as Fault Injection (FI) attacks. In practice, both types of attacks are effective means to compromise the device security. This work focuses on the attacks using laser as the light source to inject fault into logic and memory cells.

The attacks exploit the sensitivity of semiconductor devices to the visible light. For example, illuminating a transistor it is possible to switch it from a high resistance state to a low resistance state. The use of laser to inject faults into semiconductor devices was firstly introduced in 1965 [1]. Attacks using lasers belong to the semi-invasive class, i.e. it requires to perform a chip decapsulation. They can be performed through a back-side (silicon) of the chip or its front-side (metal layers). To implement back-side attacks, near-infrared (NIR) and infrared (IR) lasers are usually used. This is due to a low absorption of NIR and IR waves propagating through silicon, i.e. silicon is “transparent” to these wavelengths. The front-side attacks can be implemented with any kind of wavelength, but the optimal choice is a laser with 800 nm wavelength. To implement optical FI attack effectively various parameters should be considered, e.g. laser parameters: wavelength, its spot size, intensity and pulse duration.

Practical successful FI attacks against RSA cryptographic operations executed on a smartcard was presented in 2002 [2]. Since then various cryptographic implementations have been attacked. The overview of the optical FI attacks performed against different cryptographic algorithms as well as different cells and memories can be found in [3]. In the literature, majority of the attacks were performed through the back-side of the chip. This works reports on successful front-side optical FI attacks.

We performed the attacks using the setup available at IHP. It consists of: a 1st generation Riscure Diode Laser Station (DLS), a PC with the Riscure Inspector FI software, a stable power supply, a generator and an oscilloscope. The setup is shown schematically in Fig. 1.



*(a)* *(b)*

Fig. 1. Optical fault injection setup: *(a)* – a schematic view; *(b)* – the setup in IHP laboratory.

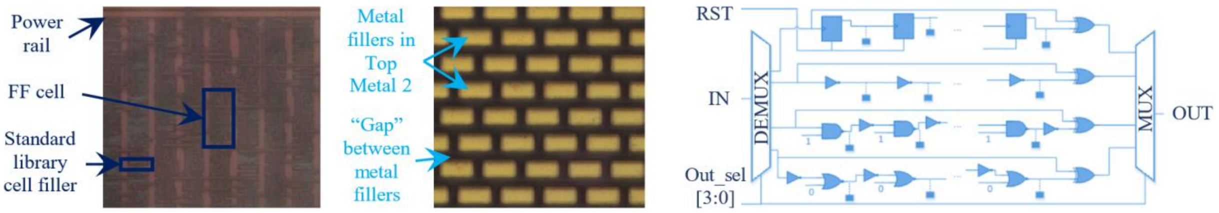
The setup can be used with three lasers: a red 808 nm single-mode laser from Alphanov, a red 808 nm and a NIR 1064 nm multi-mode lasers from Riscure. The front-side optical FI attacks were performed using the red single-mode and the red multi-mode lasers. Details about the setup parameters attacking different logic and memory cells can be found in [5]-[10].

The DLS is controlled by the Riscure software. The interaction between devices of the setup is automated by Riscure and users do not have access to it. Some parameters in the software used to perform attacks are represented in the Riscure-defined units, which are not the generally known units such as meters, seconds, etc. Clear rules for the unit conversion are not given. Thus, to ensure the repeatability of the experimental results and compliance with the promoted specifications the parameters of the setup controlled by the Riscure Inspector FI software were evaluated. The results show that evaluated minimal movement speed and minimum step size of X-Y stage, laser beam spot sizes, as well as signal controlling laser beam pulse duration differ from the values given in the corresponding documents. The non-compliance of the parameters can influence the success and the repeatability of FI attacks significantly. The knowledge about the limitations is helpful for attack planning.

The chips attacked were manufactured in two technologies: in the 130 nm and in the 250 nm IHP technology [4]. The back-end-of-line offers 3 thin metal layers and 2 thick metal layers in the 250 nm technology; and 5 thin metal layers and 2 thick metal layers in the 130 nm technology. Due to the technology requirements, the chips manufactured at IHP have metal fillers. The metal fillers are small metal areas that are placed in different metal layers between the connection wires if the required metal density of the layer is not met. Metal fillers above the cells act as obstacles for a visual inspection, i.e. they hide the internal structure of a chip and cause difficulties illuminating the cell.

*1) Chips based on standard library cells*

Attacks were performed against chips manufactured in the IHP's 250 nm (SG25H3) technology further denoted as Libval025 and in the IHP's 130 nm (SG13G2) technology further denoted as Libval013 [4]. The Libval025 chips were manufactured in an "old" IHP technology without metal fillers. Thus, the internal structure of the chip is clearly visible through the front-side. The Libval013 chips were manufactured in a recent IHP's technology with metal fillers. Fig. 2 shows the front-side of *(a)* Libval025 and *(b)* Libval013 captured using a microscope camera and *(c)* their structural scheme.


Power rail
FF cell
Standard library cell filler
Metal fillers in Top Metal 2
"Gap" between metal fillers
RST
IN
Out_sel [3:0]
DEMUX
MUX
OUT

*(a)* *(b)* *(c)*

Fig. 2. Libval chip: *(a)* – front-side of Libval025; *(b)* – front-side of Libval013; *(b)* – structural scheme.

Originally the Libval chips were designed to measure signal propagation delays through chains of inverter, NAND, NOR and flip-flop cells. To perform laser attacks the chips were placed onto Printed Circuit Board (PCB). The PCB was placed on the X-Y stage.

The attacks against Libval chips were successful in a sense that repeatable faults were injected in all 4 types of gates, i.e. flip-flop, inverter, NOR and NAND cells. According to the input of the cells the following transient faults were successfully injected: *bit-reset* ('1'→'0') faults attacking inverter, NOR and NAND cells and *bit-set* ('0'→'1') faults attacking flip-flop cells. The Libval chips manufactured in the IHP's 250 nm were successfully attacked using both red lasers. The Libval chips manufactured in the IHP's 130 nm were successfully attacked using only the red multi-mode laser. Due to the metal fillers atop the cells in Libval013 the number of successfully influenced cells is significantly reduced compared to the number of successfully influenced cells in Libval025. Using the red multi-mode laser with the increased laser beam power permanent *stuck-at* faults were injected into inverter, NAND, NOR and flip-flop cells of Libval025 chip. Details of attacks against Libval chips can be found in [5] and [10].

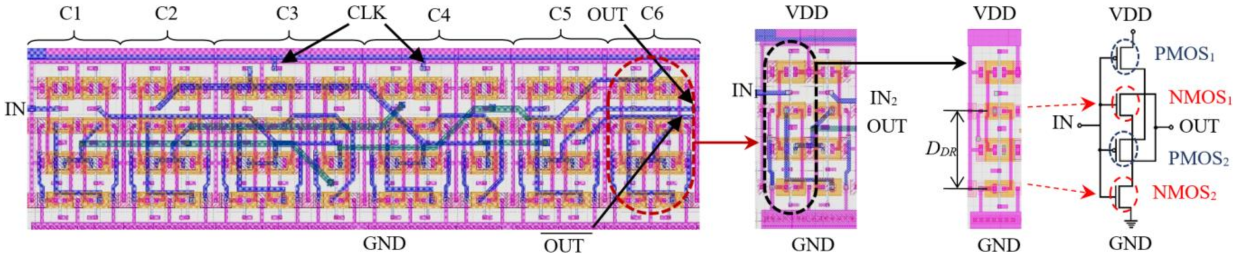
According to the layout of the cells, coordinates taken from Riscure Inspector FI software and visual observations the areas of the attacked cells, which are sensitive to optical FI attacks, were determined. The injection of faults into logic cells of Libval chips, i.e. inverter, NAND, NOR and flip-flop cells, based on 250 nm technology was feasible illuminating area where NMOS transistors are placed.

*2) Shift registers with applied radiation-hardening technique*

Attacks were performed against shift registers with hardware redundancy. Hardware redundancy is widely considered as an effective measure to increase robustness of device developed for use in harsh environments. Devices/designs with hardware redundancy are often denoted as radiation-hard. Shift registers based on two radiation-hard techniques were attacked.

*2.1) Shift registers based on Junction Isolated Common Gate (JICG) technique*

JICG technique was designed to improve total ionizing dose and to prevent single event upsets. To improve the total ionizing dose the silicide blockers are used to realize Junction Isolation (JI) of the transistor drain-source region. To prevent single event upsets the transistors are doubled. Each NMOS and PMOS transistor in a CMOS circuit is substituted by two corresponding transistors. The gates of the transistor are connected, i.e. they have a common gate (CG). To maintain a blocking capability of duplicated transistors they are placed at a distance $D_{DR}$. Each chip is a 256-bit long register, i.e. it has 256 flip-flop cells connected in series. Single flip-flop cell consists of 6 NAND cells: 2 three-input and 4 two-input NAND cells, see cells marked C+*number* in Fig. 3. Each NAND cell is based on Inverter cells, i.e. CMOS circuits, to which JICG technique is applied.



*(a)* *(b)* *(c)* *(d)*

Fig. 3. JICG cells: *(a)* – layout of JICG flip-flop; *(b)* – layout of two-input JICG NAND cell; *(c)* –layout of JICG inverter; *(d)* – an electric circuit of JICG inverter.

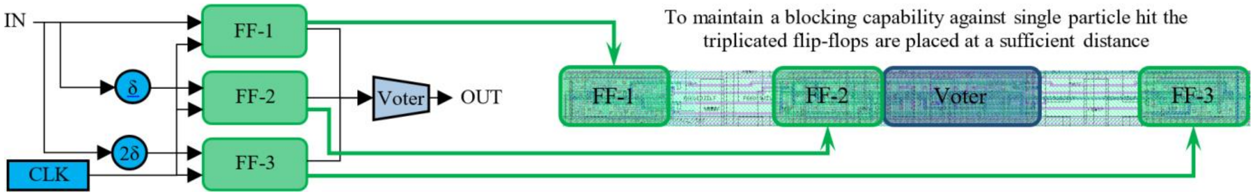
The JICG shift registers attacked were manufactured in the IHP's 250 nm technology (SGB25RH) with metal fillers and placed in package with a window. To perform laser attacks the chips were placed on the X-Y stage.

To influence the state of the flip-flop two redundant transistors have to be manipulated simultaneously. To target redundant transistors the attacks were performed applying a single laser source, i.e. it was not a multi laser attack. The "large" laser beam spot size applied in our attacks covered both redundant transistors simultaneously. According to the active input of the register, transient *bit-set* and *bit-reset* faults were successfully injected using the red single-mode laser as well as the red multi-mode laser. Performing attacks with laser beam spot sizes that do not cover two redundant transistors simultaneously were unsuccessful. No permanent faults were observed applying even maximum configurable laser beam power and pulse duration.

The injection of faults into JICG flip-flops was feasible into its NAND cells with "closed" PMOS transistors, i.e. not all NAND cells of the attacked JICG flop-flops were sensitive to the laser illumination. Depending on the logic input of the JICG flip-flop different NAND cells were sensitive to the laser illumination. Attacks details against JICG registers can be found in [6].

### *2.2) Shift registers based on Triple Modular Redundancy (TMR) technique*

The attacked TMR shift registers have been originally designed at IHP for use in space and manufactured in the IHP's 130 nm technology with metal fillers. Each manufactured chip is a 1024-bit long register where standard TMR architecture is applied for each bit, i.e. each chip has 3072 flip-flops and 1024 majority voters. The implementation attacked also has additional delay elements δ to filter short transients. Fig. 4 show *(a)* a block diagram of the part of the circuit containing 1 bit (TMR flip-flop) and *(b)* its layout.



To maintain a blocking capability against single particle hit the triplicated flip-flops are placed at a sufficient distance

*(a)* *(b)*

Fig. 4. The cell containing a bit in a TMR shift register: *(a)* – block diagram; *(b)* – layout of the cell.

To implement front-side FI attacks the chips were bonded to PCB. The PCB was placed on the X-Y stage. Attacks with small laser beam spot sizes, i.e. smaller than the distance between any two flip-flop cells, targeted at voter were unsuccessful using both lasers. Attacks with laser beam spot sizes covering at least two redundant flip-flop cells were successful. According to the active input of the register, transient *bit-set* and *bit-reset* faults were successfully injected using only the red multi-mode laser. Applying maximum configurable laser beam power and pulse duration no permanent faults were observed.

The injection of faults was feasible only when illuminating small area where flip-flop FF-2 and the voter is located. Due to the metal fillers above the TMR flip-flop as well as large laser beam spot size with unknown intensity distribution used to inject faults, it is not possible to clearly state what part of the TMR flip-flop was successfully influenced: voter or two redundant flip-flop cells. Due to the fact that attacks with small laser beam spot sizes targeted at voter were unsuccessful it is assumed that the manipulation was feasible by simultaneous influence on two flip-flops. Attack details against TMR registers can be found in [7].

### *3) Chips based on Resistive Random Access Memory (RRAM)*

Due to the ability of RRAM to store data when the power is off, i.e. non-volatility, it is of interest to realize cryptographic devices. Nevertheless, for proper data protection the RRAM cells themselves should be resistant against external malicious influence, but it is rarely investigated compared to CMOS-devices.

The IHP RRAM chips attacked were manufactured in the IHP's 250 nm technology with metal fillers using standard library cells. Each chip contains 4 kbit of memory, i.e. it has 4096 RRAM cells. Each cell is based on 1 Transistor 1 Resistor architecture, i.e. it has a transistor and a Metal-Insulator-Metal (MIM) structure. The goal of the attacks was to manipulate the state of the RRAM cell when no voltages are applied, i.e. standalone ships. To manipulate the state of RRAM cell we illuminated its MIM structure.

Manipulation of logic states of RRAM cells was feasible using both red lasers. Under the laser illumination the cells can change their logic state from the highest to the lowest one bypassing intermediate logic states. The new logic state of the attacked cell is not a transient one but will be stored in the cell. In the experiments, not only the RRAM cells illuminated directly with the laser beam, i.e. cells with gaps between metal fillers atop, but also the cells covered with metal fillers were successfully influenced. The reason of the attack success may be the well-known sensitivity of the RRAMs to temperature fluctuations. In this case the performed laser attack is a kind of a localized heating attack. To be able to use the metal fillers as a kind of countermeasure their form, placement and distribution in different metal layers have to contribute to heat dissipation. This assumption needs to be evaluated in the future. Details of attacks against IHP RRAM chips can be found in [8] and [9].

Generally, all the chips attacked in this work were successfully influenced. To prevent laser manipulations effective countermeasures have to be implemented. For example, metal fillers can be applied as optical obstacles reducing the success of front-side fault injection attacks. Based on the knowledge of the sensitive cell areas, the placement of the metal fillers can be automated in the future, i.e. the findings given in the work can serve as a basis for developing a methodology that allows to improve resistance against optical FI attacks already in the initial stage of chip development. Such methodology can be adapted for different chip manufacturing technology.

## Acknowledgment

The work was partially done in the frame of RESCUE project. This project has received funding from the European Union’s Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 722325.

## Paper Origin

This abstract is based on the following publications: [3], [5]-[10].

## References

[1] D. H. Habing, “The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits”, in IEEE Transactions on Nuclear Science, vol. 12, no. 5, Oct. 1965, pp. 91-100.

[2] S. Skorobogatov and R. Anderson, “Optical Fault Induction Attacks”, Workshop on Cryptographic Hardware and Embedded Systems (CHES), USA, San Francisco, Aug, 13–15, 2002, pp. 2–12.

[3] D. Petryk, Z. Dyka, P. Langendörfer, “Optical Fault Injections: a Setup Comparison”, Proc. PhD Forum of the 8th BELAS Summer School, Estonia, Tallinn, June 20–22, 2018, pp. 1–5.

[4] IHP Technologies for MPW & Prototyping. URL: https://www.ihp-microelectronics.com/services/research-and-prototyping-service/mpw-prototyping-service/sigec-bicmos-technologies

[5] D. Petryk, Z. Dyka and P. Langendörfer, “Sensitivity of Standard Library Cells to Optical Fault Injection Attacks in IHP 250 nm Technology”, 2020 9th Mediterranean Conference on Embedded Computing (MECO), Montenegro, Budva, June 8–11, 2020, pp. 1–4.

[6] D. Petryk, Z. Dyka, R. Sorge, J. Schäffner and P. Langendörfer, “Optical Fault Injection Attacks against Radiation-Hard Shift Registers”, 2021 24th Euromicro Conference on Digital System Design (DSD), Italy, Palermo, Sept. 1–3, 2021, pp. 371–375.

[7] D. Petryk, Z. Dyka, I. Kabin, A. Breitenreiter, J. Schäffner and M. Krstic, “Laser Fault Injection Attacks against Radiation Tolerant TMR Registers”, 2022 IEEE 23rd Latin American Test Symposium (LATS), Uruguay, Montevideo, Sept. 5-8, 2022, pp. 1-2.

[8] D. Petryk, Z. Dyka, E. Perez, I. Kabin, J. Katzer, J. Schäffner and P. Langendörfer, “Sensitivity of $HfO_2$-based RRAM Cells to Laser Irradiation”, Microprocessors and Microsystems, Volume 87, 2021, 104376, ISSN 0141-9331, pp. 1–20.

[9] D. Petryk, Z. Dyka, E. Perez, M. K. Mahadevaiaha, I. Kabin, Ch. Wenger and P. Langendörfer, “Evaluation of the Sensitivity of RRAM Cells to Optical Fault Injection Attacks”, 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenia, 2020, pp. 238-245.

[10] D. Petryk, Z. Dyka, J. Katzer and P. Langendörfer, “Metal Fillers as Potential Low Cost Countermeasure against Optical Fault Injection Attacks”, 2020 IEEE East-West Design & Test Symposium (EWDTS), Bulgaria, Varna, Sept. 4–7, 2020, pp. 1–6.

# Flicker Noise Transient Simulation, and Dose Effects Modeling Work-in-Progress

**Jan Bělohoubek**[1], **Martin Holec**[1], **Pavel Rous**[2],
**Róbert Lórencz**[1], **Tomáš Pokorný**[2], **František Steiner**[2]
[1]Czech Technical University in Prague, [2] University of West Bohemia in Pilsen
Czech Republic

{jan.belohoubek, holecma9, robert.lorencz}@fit.cvut.cz
{rousp, pokornyt, steiner}@fel.zcu.cz

**Keywords.** Flicker Noise, Electrical Simulation, CMOS, Standard Cell, SPICE, Physical Unclonable Function (PUF), Hardware True Random Number Generator (TRNG), Total Dose Effects, Ionizing Radiation

## Abstract

This work aims to support a transparent verification of the secure components of CMOS circuits [1]. The state of the work is still work-in-progress: we opened several tasks, identified open questions, and partially answered a few of them by formulating hypotheses, which are partially confirmed, but still need to be supported by more solid experimental data.

The flicker noise plays an important role in recent technology nodes. Compared to white noise, flicker noise modeling is much more complex [2], as the nature of the flicker noise changes in the short-channel device with the operating point significantly [3]. The practical method for the transient simulation incorporating flicker noise into a real CMOS circuit simulation using BSIM model parameters is not described in literature nor available to designers in a transparent way even today, despite the fact, that trusted statistical methods were developed [2]. SPICE software conventionally includes devices' flicker noise only in small-signal noise analysis.

Digital designers mostly need not care about flicker noise, as quantitative effects are embedded e.g. into noise margins, but when it comes to the design of a custom analog or mixed-signal part, transient noise simulation might become important for the design verification - e.g. in TRNG, noise (including flicker) affects the entropy. Another important aspect of flicker in CMOS is, that it is affected by aging including natural or accelerated aging [4], or total dose effects caused by ionizing radiation [5, 6], what could affect the circuit long-term reliability and security.

Transient simulation of the flicker noise is today available in established commercial VLSI tools (namely Cadence Spectre), but it represents a marginal topic even for the EDA software vendors. The algorithms are not described in the literature, and complete documentation is not available (even for customers), providing only limited insight and leaving the customer in blind trust to the software vendor, which should not be accepted in security applications, where flicker noise could play an important role. Another approach is an ad-hoc statistical approach, which is difficult and potentially error-prone. Additionally, with the advent of open-source VLSI design in the last two years, the requirements for open-source EDA, including simulation tools, arise from a wider spectrum of applications.

As a result, there is a need for support of transient flicker noise simulation in open-source EDA tools to enable fine custom design verification using available BSIM models (including typical noise

characteristics). In parallel, the effects of aging could be simulated reliably and accurately, at least in defined bounds, if the method for flicker noise parameter aging projection will be developed and validated.

This work is heavily work in progress. We developed a LUT-based model and a noise analysis BSIM model parameter extractor for transient noise simulation for Ngspice. For verification, we currently use SKY130 open-source PDK [7]. A comparison with the Cadence Spectre is currently planned. Practically, we did measurements of radiation dose effects on similar technology nodes for initial tests and basic CMOS models, and we created basic CMOS circuit models, using the developed model, matching the observed behavior providing basic confidence, that our model is able to follow observed physical effects, however further development and validation are needed. We were also able to explain experimental results by performing simulations and show when the entropy of the SRAM cell state after power-up is increased or decreased.

## Acknowledgment

The authors acknowledge the support of the OP VVV MEYS funded project CZ.02.1.01/0.0/0.0/16_019/0000765 “Research Center for Informatics”. Computational resources were supplied by the project ”e-Infrastruktura CZ” (e-INFRA LM2018140) provided within the program Projects of Large Research, Development and Innovations Infrastructures.

## References

[1] J. Lienig, S. Rothe, M. Thiele, N. Rangarajan, M. Ashraf, M. Nabeel, H. Amrouch, O. Sinanoglu, and J. Knechtel, “Toward Security Closure in the Face of Reliability Effects,” in *Proc. Int. Conf. Comp.-Aided Des*, 2021.

[2] N. J. Kasdin, “Discrete Simulation of Colored Noise and Stochastic Processes and $1/f^{\alpha}$ Law Noise Generation,” *Proceedings of the IEEE*, vol. 83, no. 5, pp. 802–827, 1995.

[3] J. Chang, A. Abidi, and C. Viswanathan, “Flicker Noise in CMOS Transistors from Subthreshold to Strong Inversion at Various Temperatures,” *IEEE Transactions on Electron Devices*, vol. 41, no. 11, pp. 1965–1971, 1994.

[4] P. F. Butzen, V. Dal Bem, A. I. Reis, and R. P. Ribas, “Design of CMOS Logic Gates with Enhanced Robustness Against Aging Degradation,” *Microelectronics Reliability*, vol. 52, no. 9-10, pp. 1822–1826, 2012.

[5] H. Barnaby, “Total-Ionizing-Dose Effects in Modern CMOS Technologies,” *IEEE transactions on nuclear science*, vol. 53, no. 6, pp. 3103–3121, 2006.

[6] I. S. Esqueda, H. J. Barnaby, and M. L. Alles, “Two-Dimensional Methodology for Modeling Radiation-Induced Off-State Leakage in CMOS Technologies,” *IEEE transactions on nuclear science*, vol. 52, no. 6, pp. 2259–2264, 2005.

[7] S. P. Authors. (2020 – 2021) SkyWater SKY130 PDK’s documentation. [Online]. Available: https://skywater-pdk.readthedocs.io/en/latest/

# How to measure high-speed network: a case study

Tomas Benes, Jaroslav Pesek, Tomas Cejka
*Faculty of Information Technology, Czech Technical University in Prague & CESNET a.l.e.*
*Thakurova 9 & Generala Piky 430/26, Praha 6*
{benesto3, jaroslav.pesek, tomas.cejka}@fit.cvut.cz

**Abstract**

High-speed ISP networks are usually monitored using IP Flows. This feasible and scalable approach provides enough high-level information about the situation in the network and supports various use cases, such as the detection of unusual events like operational outages or security threats. The paper introduced by this extended abstract presents the monitoring architecture, the created dataset, and detailed statistics of public network traffic measured in the ISP backbone using a scalar aggregation method based on IP flows. Such insight into traffic enables future design and development of hardware optimizations, tuning the performance of monitoring systems and adapting security detection algorithms for target environments. Furthermore, the described open-source tools can be deployed for long-term aggregation flow-based monitoring even in large networks.

***Keywords*— traffic monitoring; IP flows; traffic statistics; heavy-tailed distribution; flow cache; ISP network**

## I. Introduction and Motivation

With evolving speeds of computer networks, analysts deal with bigger and bigger data. Every researcher and developer of an application dealing with a large amount of network data must understand the shape and characteristics of the traffic to consider possible optimizations and limits. That is why we study and exploit network monitoring tools to retrieve a detailed but long-term insight into the traffic of wide area networks. Our methodology can be used in any network to get an overview of its properties. We have chosen one of the most challenging types of network — an ISP network that deals with a tremendous amount of data and needs to comply with the privacy standards of the ISP.

## II. Measuring and measuring architecture

### A. Flow monitoring

The flow-based approach to monitoring was explained in detail, e.g., by Hofstede et al. in [1]. The commonly used representation of flow data is currently Netflow [2] or IPFIX format [3]. Nowadays, there are two ways of aggregating the packets into sets based on the direction of the communication: Unidirectional flows and bidirectional flows (biflows) [4]. We aim to use the latter one.

### B. Architecture

Measurements were performed using open-source tools composed into a scalable monitoring infrastructure, as shown in Fig. 1. The monitoring pipeline starts with an IP flow exporter that computes IPFIX data processed in real time. Since we aimed to compute a wide range of statistics, which requires a lot of computational resources, we designed a configuration to perform the online processing in parallel. For our needs, an open-source set of tools was created[1].

This makes a flow-based architecture well-suited to our detailed monitoring and analysis needs and can be scaled for large networks. The components of the monitoring pipeline are briefly described in the following sections.

[1] https://github.com/CESNET/flowcache-measurement

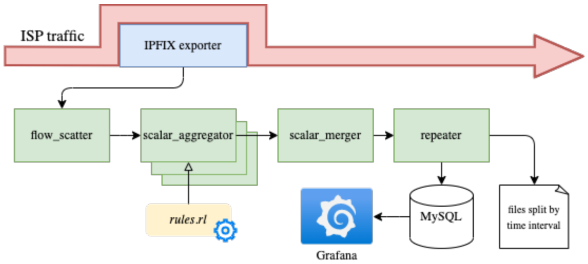


Figure 1: Architecture of measuring pipeline.

Table I: ipfixprobe important flow features and their descriptions

| IP Flow Feature | Description |
|---|---|
| BYTES | Total number of bytes in the flow |
| PACKETS | Total number of packets in the flow |
| SRC_IP | The IP address from which the flow originated |
| DST_IP | The IP address to which the flow is destined |
| SRC_PORT | The port of the originating device |
| DST_PORT | The port of the destination device |
| PROTOCOL | The L4 protocol used for the flow (e.g., TCP, UDP) |
| TIME_FIRST | Timestamp of the first packet in the flow. |
| TIME_LAST | Timestamp of the last packet in the flow. |
| FLOW_KEY | Flow key for unidirectional flow |
| TCP_FLAGS | TCP flags if TCP protocol is used |

Table II: Describtion of network traffic volumes (flows, bytes, packets) for different periods (day/night, weekday/weekend).

| | | **Flows [MFlows]** | | | | | **Bytes [GB]** | | | | | **Packets [KPackets]** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **Mean (SD)** | **Min** | **$Q_1$** | **$Q_3$** | **Max** | **Mean (SD)** | **Min** | **$Q_1$** | **$Q_3$** | **Max** | **Mean (SD)** | **Min** | **$Q_1$** | **$Q_3$** | **Max** |
| **Day** | **Weekday** | 82.27 (25.65) | 13.87 | 66.88 | 101.57 | 243.92 | 69.97 (22.40) | 10.73 | 56.39 | 86.54 | 215.66 | 1.56 (0.79) | 0.48 | 1.00 | 1.82 | 5.83 |
| | **Weekend** | 38.30 (12.13) | 10.68 | 30.17 | 44.64 | 88.44 | 32.52 (10.02) | 7.76 | 26.06 | 37.69 | 88.40 | 0.70 (0.79) | 0.44 | 0.59 | 0.74 | 3.15 |
| **Night** | **Weekday** | 34.21 (21.36) | 7.54 | 17.07 | 46.63 | 108.10 | 28.50 (17.92) | 5.37 | 14.09 | 39.64 | 98.32 | 0.89 (0.72) | 0.38 | 0.51 | 0.84 | 3.67 |
| | **Weekend** | 27.69 (17.73) | 8.38 | 14.43 | 37.01 | 93.43 | 23.28 (14.76) | 5.54 | 12.07 | 31.59 | 98.58 | 0.59 (0.36) | 0.38 | 0.47 | 0.59 | 3.27 |

*1) Flow exporter:* We employed `ipfixprobe`[2], which is an open-source flow exporter developed by the CESNET association in collaboration with Czech Technical University in Prague and Brno University of Technology. The monitoring pipeline starts with an IP flow exporter that computes IPFIX data processed in real time. The list of input features computed by the exporter is enumerated in Table I.

*2) Aggregation:* In our study, we employ a scalar aggregation (included in the NEMEA system [5]) to analyze the input features and compute statistics to describe the properties and behaviour of the traffic. It is a special case of an aggregation process in time, where the output is a single vector of statistics per each time window of one minute.

*3) Scalability:* The scalar aggregation contains complex operations such as *COUNT_UNIQ, COUNT, etc.*. With many aggregation rules defining statistics, it is necessary to apply parallel computation to sustain the throughput of the monitoring pipeline. This is achieved by splitting the input flow stream among *N* equal parts using the flow scatter module of the NEMEA system. The results are retrieved by the scalar merger module of NEMEA, which applies appropriate functions to process partial results; during our measurement, we used 8 parallel processes to compute the statistics and aggregate the traffic from the network.

*4) Output:* The computed statistics are efficiently stored in a classic relational database. Structured database storage allows for robust data management and efficient querying, which is crucial when dealing with extensive network traffic data. The database provides fast and reliable access to the data during analysis and visualization.

### *C. Environment*

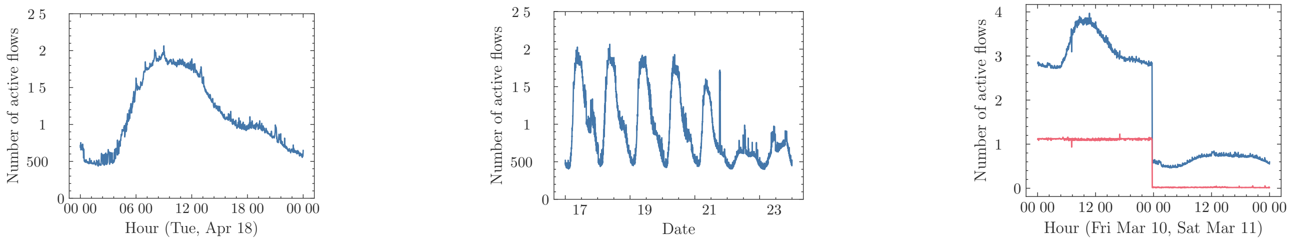
Our measurement was conducted in CESNET2, the national research and education network in the Czech Republic. It interconnects many academic institutions, research organizations, governmental offices, and others. It represents around 500,000 users. There are six monitoring probes at the infrastructure perimeter, equipped with special hardware cards with FPGA to accelerate the pre-process packets and software flow exporter `ipfixprobe` to aggregate IP flows and export them to a flow collector. Measurement for the paper was performed from February 25th 2022 to May 3rd 2022, using the monitoring probe that observes one of the lines to the Czech internet exchange point (NIX.CZ), which carries most of the public traffic of CESNET2.

## III. Analysis

We demonstrate the differences in traffic during weekdays, weekends, days, and nights with basic statistics measures in Table II. In all measurements, we define the following periods as follows. The day is defined as 6 to 20 hours of local time; otherwise, there is a night. The weekday is defined as commonly understood Monday till Friday; otherwise weekend.

When we mention the number of flows, we always refer to the number of active flows, ergo the number of overlapping flows in a given time window. Flow exporters can sometimes increase the number of flows by using something called inactive timeouts for the flows they export. Most of these flows are UDP flows, which do not have the connection-ending condition. Because flow exporters work this way, the count of flows always shows the toughest situation on the network. It's crucial to know about this to understand the results properly. This measure should give a more accurate picture of network applications compared to the often-used flows per second, which can make the actual network traffic seem different than it really is.

[2] https://github.com/CESNET/ipfixprobe



(a) One day

(b) One week.

(c) Possible SYN flood.

Figure 2: A zoom for small parts – one day, one-week perspective and an inspection of SYN flood event that occurred during our measurement.

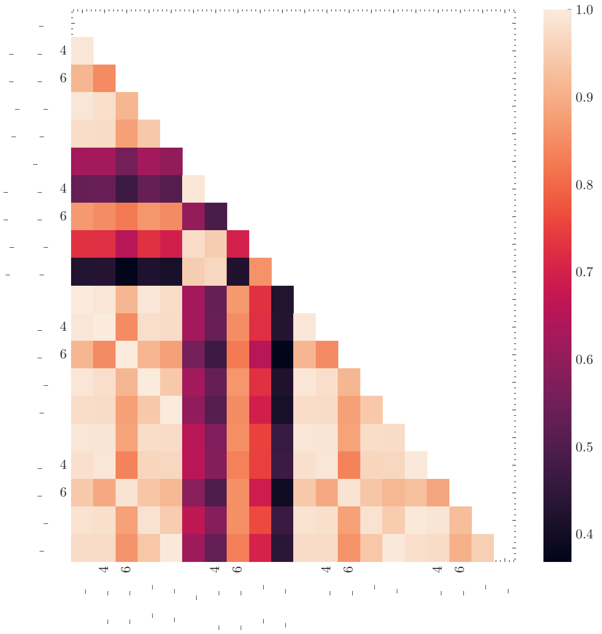
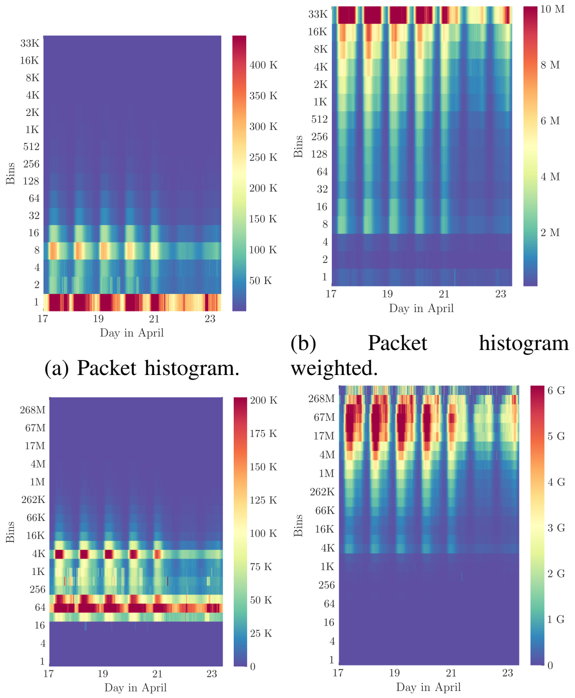


Figure 3: A heatmap showing relationships between relevant features employing Pearson's correlation coefficient. We can see that most volume-based (packet, bytes) features evince a strong correlation with each other. However, they do evince a weak correlation to the flow-based features containing information about a number of active flows (features with the prefix no_flows). This may lead to incorrect usage of the flow-based features to make assumptions about the volume transferred throughout the network.



(a) Packet histogram.

(b) Packet histogram weighted.

(c) Bytes histogram.

(d) Bytes histogram weighted.

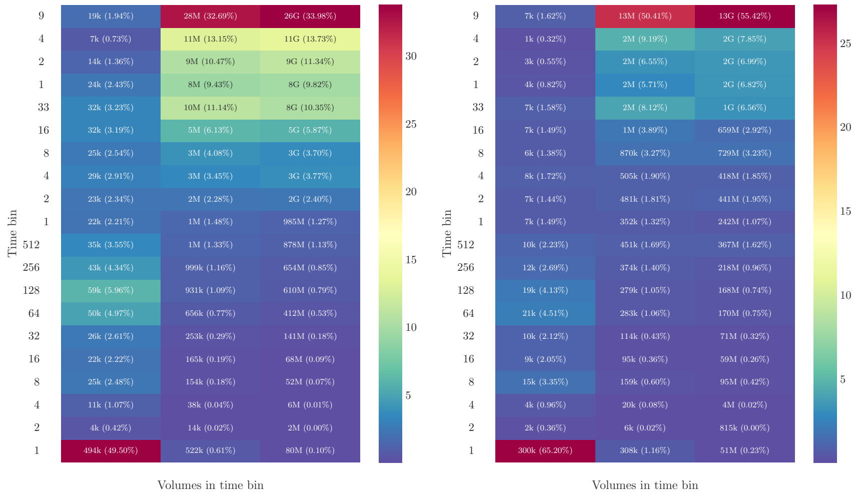
Figure 4: Relative and not relative view on histograms of packets and bytes in flows. We can see that most flows are very light in the sense of packets and bytes, but if we look at a relative view, the centre of gravity is different; most of the weight in the sense of the number of packets and data throughput lies in very small flows.

Graphs in Figure 2 represent a progression of the number of active flows throughout the day (2a) and week (2b). We can effortlessly distinguish days, weekdays, and weekends. The last figure (2c) shows a period during a suspected DDoS attack using SYN flood. It shows an increase of around 2M flows per time window, from which 1M are TCP flows containing only SYN packets (flows with only 1 packet).

In addition to the usual volumetrics, we also analyzed how individual features interact. For this, we chose the well-known Pearson correlation coefficient, which shows how individual random variables correlate. In Figure 3, we can see that the least correlating variables are the flow-based group and volume-based group consisting of packet and byte variables. This is a sign that statistics based on flow only cannot be used to describe the traffic on a network very well. Therefore the appropriate performance metrics for a network application should be a set of a number of active flows and packets per second instead of only flows per second. A demonstration of why these groups of variables do not correlate can be seen in Figure 5. In the histograms, we can see the percentage distribution of flows, packets and bytes in relation to the flow duration of their associated flow. The first column represents the flow-based group and shows us that over 50% of the flows on the network are shorter than 16 ms. However, the other two represent the volume-based group and show us that more than 50% of the packets and bytes are contained in flows that are longer than 16 s, which is around 5–7% of all flows.

Another way to visualize this phenomenon is to use a weighted view instead of creating a histogram in relation to the flow duration. The weighted view throughout one week of our measurement can be seen in Figure 4. The weighted view is simply multiplying occurrence by the bin value instead of just counting it as a single occurrence. This allows us to see that most weight lies in very few flows. In Figure 5, we have included detailed analyses of a single window in the middle of the day and the middle of the night. We see that the total volumes are weaker at night than during the day — at night, we can see the same exact effect of the heavy-tail distribution of the traffic.

The last insight is into SYN-only communication. We found that the SYN flood traffic is almost exclusively generated during weekdays, as visualised in Figure 6. This makes logical sense that the SYN flood traffic is designed to overwhelm the service during the highest demand for the target.



(a) Window in the middle of the day.

(b) Window in the middle of the night.

Figure 5: A detailed view of a single 1-minute window in the middle of the day and the middle of the night. The view contains distributions of the flows, packets and bytes in relation to the duration of the associated flow. We can see the heavy-tailed character of the packets and the data in the transmissions

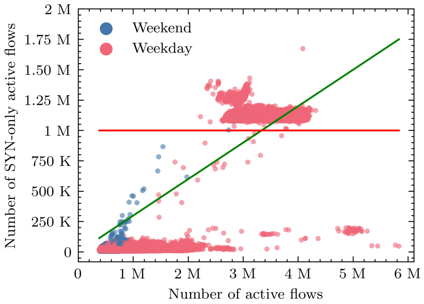


Figure 6: We offer two views on SYN flood analysis. We set the threshold of 30% of SYN-only flows in a portion of a number of active flows per time window of one minute (separated by a green line — above the line, the window contains more than 30% of SYN-only flows). The second view is based on the absolute value — above the red line; the window contains more than 1M of SYN-only flows. In both cases, we observe that only weekdays are above the thresholds on a massive scale.

## IV. Conclusion

This abstract briefly introduced our work and shared some of our findings and insights. In the full paper, we go much deeper into the solution's analysis, inference, and architecture. This has resulted in a set of generic tools that can be deployed behind any exporter that uses the IPFIX format. At the same time, as a by-product, a unique dataset was created in the sense that it captures long continuous periods without any traffic sampling or dropouts and also, the capture was retrieved on a high-speed network with an extensive user base.

## Acknowledgment

This research was funded by the Ministry of Interior of the Czech Republic in the project "Flow-Based Encrypted Traffic Analysis" (VJ02010024).

## Paper Origin

This extended abstract's origin is a full paper submitted to the CNSM 2023 conference.

## References

[1] R. Hofstede *et al.*, "Flow monitoring explained: From packet capture to data analysis with NetFlow and IPFIX," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 2037–2064, 2014, Conference Name: IEEE Communications Surveys Tutorials, ISSN: 1553-877X. DOI: 10.1109/COMST.2014.2321898.

[2] B. Claise, *Cisco systems NetFlow services export version 9*, Number: 3954 Series: Request for comments tex.howpublished: RFC 3954 tex.pagetotal: 33, Oct. 2004. DOI: 10.17487/RFC3954. [Online]. Available: https://rfc-editor.org/rfc/rfc3954.txt.

[3] P. Aitken *et al.*, *Specification of the IP flow information export (IPFIX) protocol for the exchange of flow information*, Number: 7011 Series: Request for comments tex.howpublished: RFC 7011 tex.pagetotal: 76, Sep. 2013. DOI: 10.17487/RFC7011. [Online]. Available: https://rfc-editor.org/rfc/rfc7011.txt.

[4] B. Trammell *et al.*, *Bidirectional flow export using IP flow information export (IPFIX)*, Number: 5103 Series: Request for comments tex.howpublished: RFC 5103 tex.pagetotal: 24, Jan. 2008. DOI: 10.17487/RFC5103. [Online]. Available: https://rfc-editor.org/rfc/rfc5103.txt.

[5] T. Čejka *et al.*, "NEMEA: A framework for network traffic analysis," in *2016 12th International Conference on Network and Service Management (CNSM)*, Montreal, QC, Canada: IEEE, Oct. 2016, pp. 195–201. DOI: 10.1109/CNSM.2016.7818417. [Online]. Available: http://ieeexplore.ieee.org/document/7818417/ (visited on 03/14/2022).

# Equivalent Keys as a Side-Channel Countermeasure for the Rainbow Signature Scheme

David Pokorný, Petr Socha, Martin Novotný
*Czech Technical University in Prague, Faculty of Information Technology, Department of Digital Design*
*Thákurova 9, Prague 6*
{david.pokorny, petr.socha, novotnym}@fit.cvut.cz

## Abstract

Algorithms based on the hardness of solving multivariate quadratic equations present promising candidates for post-quantum digital signatures. Contemporary threats to implementations of cryptographic algorithms, especially in embedded systems, include side-channel analysis, where attacks such as differential power analysis allow for the extraction of secret keys from the device's power consumption or its electromagnetic emission. To prevent these attacks, various countermeasures must be implemented. In this paper, we propose a novel side-channel countermeasure for multivariate quadratic digital signatures through the concept of equivalent private keys. We propose a random equivalent key to be generated prior to every signing, thus randomizing the computation and mitigating side-channel attacks. We demonstrate our approach on the Rainbow digital signature, but since an unbalanced oil and vinegar is its special case, our work is applicable to other multivariate quadratic signature schemes as well. We analyze the proposed countermeasure regarding its properties such as the number of different equivalent keys or the amount of required fresh randomness, and we propose an efficient way to implement the countermeasure. We evaluate its performance regarding side-channel leakage and time/memory requirements. Using test vector leakage assessment, we were not able to detect any statistically significant leakage from our protected implementation.

***Keywords*— embedded systems, multivariate quadratic signature, post-quantum cryptography, side-channel security**

## ACKNOWLEDGMENT

This research was funded by the Ministry of the Interior of the Czech Republic Grant Number VJ02010010, "Tools for AI-enhanced Security Verification of Cryptographic Devices" in the program Impakt1 (2022–2025). The authors thank David Kokoška, Jan Onderka, and Vojtěch Miškovský for valuable discussions.

## PAPER ORIGIN

The presented work was originally published in [1].

## REFERENCES

[1] Pokorný, D., Socha, P., & Novotný, M. (2022). Equivalent Keys: Side-Channel Countermeasure for Post-Quantum Multivariate Quadratic Signatures. Electronics, 11, 3607.

## Sponsors

### Czech Technical University in Prague

The conference has been sponsored by the CTU project SVK 62/23/F8.

### Research Center for Informatics

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

### ASICentrum

ASICentrum, established in 1992 in Prague is a design center of EM Microelectronic and a competence center of ETA, belonging to the Swatch Group. EM Microelectronic is one of the most innovative IC providers. It developed and manufactured the smallest and the lowest power consuming Bluetooth chip on the market, the top performing optical sensors for optical office as well as gaming mice and it was the first to release the award-winning world-first dual-frequency NFC + RAIN RFID emlecho.

### CISCO

With networking, security, collaboration, cloud management, and more, Cisco helps to securely connect industries and communities. TD&R Data Science team in Prague is developing complex systems for network and cross domain detections using machine learning and artificial intelligence. We build cloud-based solutions for detecting threats from diverse types of telemetry sources. We analyze data of many millions of devices all over the world.

### Institute for Support of Innovative Education

We are here for Czech innovative and alternative initiatives in education to create supportive conditions for them. We provide consultations about creation and management of schools, we map educational innovators and related organizations, we mediate contact, we try our own or external educational innovations and we help to adopt those successful ones in common educational practices.

### METIO Software

Metio Software is a software development company that develops various kinds of software projects.

### STMicroelectronics

STMicroelectronics is a world leader in providing the semiconductor solutions that make a positive contribution to people's lives, today and into the future. ST is a global semiconductor company with net revenues of US$ 8.35 billion in 2017. Offering one of the industry's broadest product portfolios, ST serves customers across the spectrum of electronics applications with innovative semiconductor solutions for Smart Driving and the Internet of Things. By getting more from technology to get more from life, ST stands for life.augmented.

### SYSGO

SYSGO is the leading European provider of real-time operating systems for critical embedded applications. Our products have been designed to meet the highest requirements when it comes to Safety and Security. Our customers are leading players in the Avionics & Defense, Space, Railway, Automotive and Industrial Automation and Medical industries, who use our PikeOS product as a platform for critical systems that need to be certified against industry-specific Safety and Security standards.

## Partners

### IMA

MA is a Czech ICT company specializing in the areas of identification, location detection, evidence and Internet of Things. IMA has a long-standing profile as an independent centre focused on the development and application of microcomputer electronics. In 2017, IMA started working with the German company WITTE Automotive on innovative gesture recognition systems. WITTE Automotive Group, of which IMA became a full partner on January 1, 2021, is a leader in the field of mechatronic locking systems and a major business group with a global presence. Our systems are used daily by hundreds of thousands of people worldwide by customers such as Škoda Auto, ČVUT, ČEZ, mBank, LEGO ... We develop smart and innovative identification solutions and always strive to stay a few steps ahead of the competition. Participation in international grant projects aimed at finding new useful solutions for the future helps us to do this.

### IEEE Student Branch at Czech Technical University in Prague

### IEEE Young Professionals

### Computer (C) Society Chapter of the Czechoslovakia Section of IEEE

## Partner conferences

### 28th IEEE European Test Symposium 2023