Blansko Summer School 2020

Overview of ongoing research

Bruno Rossi
brossi@mail.muni.cz

Lasaris, Faculty of Informatics, Masaryk University

Aug 31, 2020

CyberPhysical Sytems (CPS)

- A **cyber physical system (CPS)** is a collection of computing devices communication with one another and interacting with the physical world via sensors and actuators in a feedback loop.
- A CPS is a generalization of an embedded system.
- Key differences of CPS compared to traditional systems:
  - **Reactive computation**: input and outputs impact on the physical world passing through the cyber world (e.g. sequences of commands that change the force applied to the throttle to have a specific acceleration)
  - **Concurrency**: is fundamental in CPS (e.g. swarm of robots exchanging information)
  - **Feedback Control of the physical world**: control systems interact with the physical world via sensors and influence the outcome with actuators.
  - **Real time computation**: modelling time delays, time-dependent coordination protocols, impact of correctness and performance

Safety -critical Cyber Physical Sytems (CPS)

- A **safety-critical cyber physical system (CPS)** is the one that is employed for **safety-critical applications**, that is where the safety of the system has higher priority over the design objectives such as performance and development costs.
- Ensuring that the system works correctly at design time is of paramount importance: the traditional approach of **system design, development testing and validation** might be surpassed in this area by **formal modelling and validation**.

C4e Research Programme

A multidisciplinary centre of Masaryk university that brings together expert academic departments to address complex cyberspace problems.

Involved experts collaborate and carry out multidisciplinary excellence research and development within the research programmes. Their research results immediately reflect in their educational activities.

The centre aims at practical application of research activities. To this end, we collaborate with a wide range of public and private sector partners.

- Critical Information Infrastructures Protection, lead by Tomáš Pitner.
  (1) Simulation and predictive analysis of critical infrastructures
  (2) Formal verification of critical infrastructures
  (3) Recommendations for critical infrastructure realization
- Cybersecurity, lead by Pavel Čeleda.
  (1) Simulation of advanced attacks and efficient defence
  (2) Advance analysis of operational data
  (3) Similarity management for big-data analytics
- Law, lead by Radim Polčák.
  (1) cybersecurity law
  (2) law of cyber-defence
  (3) cybercrime law

The Centre is managed by the director Roman Čermák.

Subprogramme 3 Goals

Recommendations for critical infrastructure realization

- **Goal:** provide recommendations related to the implementation of critical infrastructures based on quality perspectives (security, safety, reliability, robustness, privacy, legal topics).
- Expected Research Results:
  - **RR1.** Models of critical infrastructures and related processes relevant for the resolution of critical situations in the field of cyber-security.
  - **RR2.** Key guidelines for the design, realization and control of critical cyber-physical systems.

Subprogramme 3 Team

Bruno Rossi, FI MU

Renate Motschnig, Universität Wien

Radek Ošlejšek, FI MU

Gerald Quirchmayr, Universität Wien

Subprogramme 3 Results

Recent Results

- **Behavior analysis of cybersecurity training programs.** Improve training programs of the protection of critical information infrastructures using techniques of process mining **(RR1,RR2)**.
- **Risk management** for Smart Grids Infrastructure **(RR2)**.
- **Usage of co-simulations in the context of Smart Infrastructures (Smart Grids, specifically microgrids).** modelling “what-if” scenarios deriving common scenarios related to changes of topologies of the distribution nodes **(RR2)**.
- **Visualization surveys** for cyber exercises and **software development models** to take into account cybersecurity aspects **(RR2)**.

Ex1. Recommendations for Smart Grid Security Risk Management

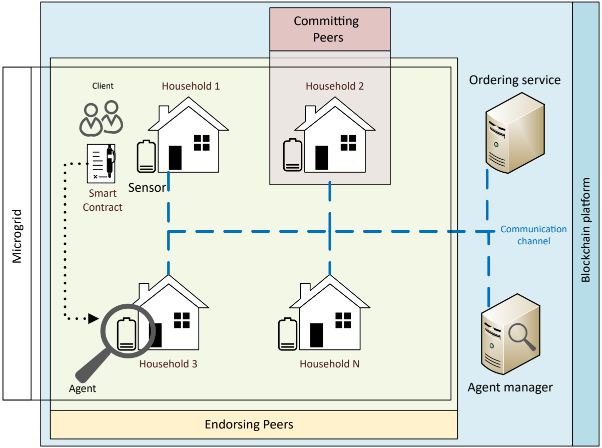
- **Goal:** Provide recommendations tailored for Smart Grids Security Management.
- We provided a tailored model for SG cybersecurity more specific than NIST Framework for Improving Critical Infrastructure Cybersecurity - taking activities from existing frameworks in the SG domain.

Table 3. Recommendations for security risk assessment (SRA).

SRA tasks		Recommended activities
SRA 1	Defining the purpose and scope of risk assessment	• Proactive and automated tools
SRA 2	Conduct threat, vulnerability, and impact analysis	• Threat profiles and models
		• Security advisories
		• Vulnerability catalogues
		• Vulnerability scanning tools
		• Impact matrix
		• Impact assessment reports
SRA 3	Development of a risk model	• Probabilistic models
		• Attack tree models
		• Intrusion detection models
		• State estimation models
		• Risk taxonomy
SRA 4	Risk determination	• Risk matrix and risk scales
		• Graph-theoretic approaches
		• Stochastic approaches
		• System-theoretic approaches
SRA 5	Continuous monitoring and update of risk assessment	• Periodic risk assessment
SRA 6	Communication and documentation of risks	• Risk assessment reports
		• Risk registers

Ex2. Blockchain SG - with Bacem, Stano

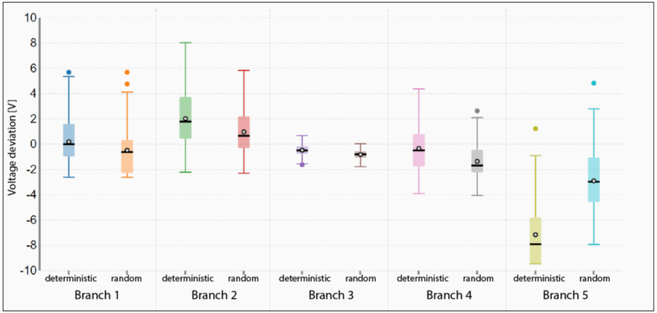
- **Goal:** Investigating the usage of Blockchain for Microgrids energy transactions between prosumers.

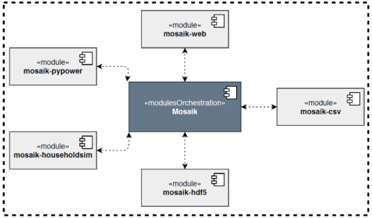


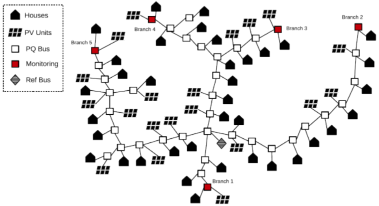
Ex3. Co-simulations in Smart Grids

- **Goal:** Investigating the usage of co-simulations for what-if scenarios in Smart Grids.

We simulate a **failure/attack**: five PV units are shut down **randomly** and **deterministically**







Results: the modified Mosaik platform can be used to simulate dynamically changing scenarios, based on changes to the topology of the network.

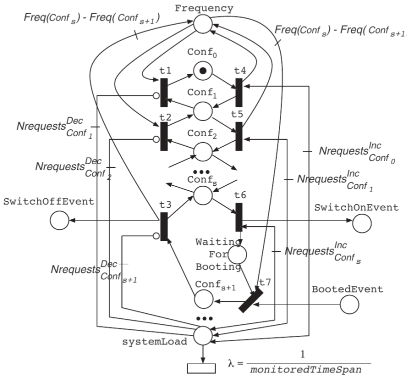
Ex4. Petri Nets usage in SG - with Bacem, Stano, Mouzhi

- **Goal:** Provide an overview of the usage of Petri Nets in modelling Smart Grids.

4.3 Reliability

Table 3. Usage of Petri Nets for Reliability analysis (4.3)

Reference	Year	Topic	PN Type
Liu et al. [25]	2010	Fault identification and diagnostics	General
Zeng et al. [50]	2011	Dependability analysis, substation attack modelling	GSPN
Saki et al. [36]	2011	Failure diagnostics, monitoring	General
Calderaro et al. [3]	2011	Failure identification and diagnostics	General
Zeng et al. [51]	2012	Dependability analysis, substation attack modelling	GSPN
Diekhake and Schneider [10]	2013	Monitoring	Causal PN
Wang et al. [42]	2014	Fault diagnostics	Directional weighted fuzzy PN
Wang et al. [40]	2014	Dependability analysis	SPN
Wang et al. [41]	2015	Fault diagnostics	General
Ghasemieh et al. [14]	2015	Resilience and survivability analysis	Hybrid PN
Chen et al. [6]	2015	Detection of nontechnical losses, outages, illegal and fault events	Fuzzy PN
Panchal and Kumar [32]	2016	Reliability and risk analysis	General
Hüels and Remke [15]	2016	Resilience, battery management analysis	Fluid SPN
Marrone and Gentile [28]	2016	Resilience, energy management	Fluid SPN
Matos and Sanchez [29]	2016	Fault tolerance, fault recovery	Hybrid PN
Morris et al. [30]	2017	Availability and resiliency analysis	SRN
Mahdi et al. [27]	2017	Reliability and availability analysis	SPN
Sreerama and Swarup [37]	2017	Fault localization and diagnostics	General
Jiang et al. [17]	2018	Fault detection, diagnostics and recovery	General
Li et al. [22]	2018	Reliability analysis, topology attacks	General



source example: Perez-Palacin, D., Mirandola, R., & Merseguer, J. (2012). QoS and energy management with Petri nets: A self-adaptive framework. Journal of Systems and Software, 85(12), 2796-2811.

Ex5. Code Quality issues - with Stano, Martin

- **Goal:** Understand the impact of code quality in the context of CPS development.

Comparing Maintainability Index, SIG Method, and SQALE for Technical Debt Identification

PETER STREČANSKÝ, Masaryk University
STANISLAV CHREN, Masaryk University
BRUNO ROSSI, Masaryk University

There are many definitions of software Technical Debt (TD) that were proposed over time. While many techniques to measure TD emerged in recent times, there is still not a clear understanding about how different techniques compare when applied to software projects. The goal of this paper is to shed some light on this aspect, by comparing three techniques about TD identification that were proposed over time: i. the Maintainability Index (MI), ii. SIG TD models and iii. SQALE analysis. Considering 20 open source Python libraries, we compare the TD measurements time series in terms of trends and evolution according to different sets of releases (major, minor, micro), to see if the perception of practitioners about TD evolution could be impacted. While all methods report generally growing trends of TD over time, there are different patterns. SQALE reports more periods of steady states compared to MI and SIG TD. MI is the method that reports more repayments of TD compared to the other methods. SIG TD and MI are the models that show more similarity in the way TD evolves, while SQALE and MI are less similar. The implications are that each method gives slightly a different perception about TD evolution.

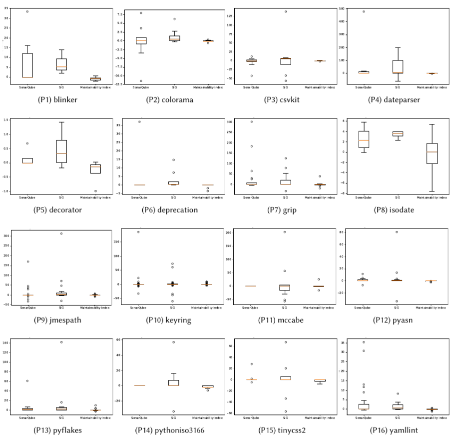
Additional Key Words and Phrases: Software Technical Debt, Software Maintenance, Software Quality, Maintainability Index, SIG Method, SQALE

ACM Reference Format:
Peter Strečanský, Stanislav Chren, and Bruno Rossi. 2020. Comparing Maintainability Index, SIG Method, and SQALE for Technical Debt Identification. 1, 1, Article 4 (August 2020), 19 pages. https://doi.org/xx.xxx/xxx_x

1 INTRODUCTION

Technical Debt (TD) is a metaphor introduced by Ward Cunningham in 1993 [6]. Cunningham compared poor decisions and shortcuts taken during software development to economic debt. Even though these decisions can help in the short-term, such as speeding-up development or the release process, there is an unavoidable cost that will have to be paid on the long term in terms of re-development and increased complexity for the implementation of new features, not to mention possible defects and failures.

The fundamental of this metaphor, however, was shaped in the 80s, when Lehman introduced the laws of software evolution [27]. The second law states that *"as a system evolves, its complexity increases unless work is done to maintain or reduce it"*. Even though this metaphor was coined more than two decades ago (and almost 40 years passed since the



(P1) blinker (P2) colorama (P3) csvkit (P4) dateparser
(P5) decorator (P6) deprecation (P7) grip (P8) isodate
(P9) jmespath (P10) keyring (P11) mccabe (P12) pyasn
(P13) pyflakes (P14) pythoniso3166 (P15) tinycss2 (P16) yamllint

Recent Publications

.:Accepted/Published:.

- Ošlejšek, R., Rusnák, V., Burská, K., Švábenský, V., Vykopal, J. and Cegan, J., 2020. **Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training**. IEEE Transactions on Visualization and Computer Graphics (TVCG) – IF 3.078.
- Ošlejšek, R. and Pitner, T., 2020. **Optimization of Cyber Defense Exercises Using Balanced Software Development Methodology**. International Journal of Information Technologies and Systems Approach – IF 0.18.
- Motschnig, R., Silber, M. Švábenský, V. **How Does a Student-Centered Course on Communication and Professional Skills Impact Students in the Long Run?**, Frontiers in Education (FIE) 2020, IEEE.
- Mbarek, B., Chren, S., Rossi, B. and Pitner, T., 2020, April. **An Enhanced Blockchain-Based Data Management Scheme for Microgrids**. In WAINA2020 (pp. 766-775). Springer.
- Strečanský, P., Chren, S. and Rossi, B., 2020. **Comparing maintainability index, SIG Method, and SQALE for technical debt identification**. In Proceedings of the 35th Annual ACM Symposium on Applied Computing (pp. 121-124).
- Strečanský, P., Chren, S., Rossi, B. **– (Invited extended version)**, Scientific Programming, 2020 – IF 1.2.

Future Publications

.:WiP:.

- Ošlejšek, Macák, Bühnová. **Cybersecurity Training Session Analysis using Process Mining** - under preparation, conference paper.
- Zákopčanová, Kouřil, Hrdina, Beran, Ošlejšek. **Fimetis: Visualizations and Data Analysis for Digital Investigation** - under preparation, conference paper.
- Motschnig, R., Silber, M. Švábenský, **Extension of FIE article** for IEEE Transactions on Communication.
- Burská, K., Rusňák, V., Ošlejšek. R. **Data-driven Insight Into the Puzzle-based Cybersecurity Training** submitted to conference.
- Mihal, P., Schvarcbacher, M., Rossi, B., Pitner, T. **Smart Grids Co-Simulations: State of Research**. Submitted to Elsevier Sustainable Computing – IF 1.8.
- Mbarek, B., Chren, S., Rossi, B., Pitner, T. **A Hyperledger Fabric Blockchain-based Electricity Trading Model in Microgrids** submitted to Elsevier Journal of Pervasive and Mobile Computing – IF 2.7.
- Gryga, L., Rossi, B. **Co-Simulation of Smart Grids: Dynamically Changing Topologies in Failure Scenarios**, to be submitted to FEDCSIS2020.

Future Plans

- Collection of detailed data capturing the behavior of participants of **cybersecurity training sessions**. **Reconstruction of users' walkthroughs** from this data using process mining methods.
- Usage of **co-simulations** in the context of Smart Infrastructures (Smart Grids, specifically microgrids) to simulate different layers of the infrastructure.
- Collection of recommendations about **cyber-qualification programs** to build profiles for cyber-training.
- Studying generic **competence models** to see how these can be useful for cyberqualifications. Furthermore, studying competence models for digital literacy and investigating how a **zero-outage culture** can be approached in (ICT-)organizations.
- Joint paper with other participants of the C4E, subprogram 3 – a survey paper mapping existing **simulators of critical infrastructures** and their properties (models of CII supported, learning features available, data analysis support, ...).

MUNI
C4E

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

MINISTRY OF EDUCATION,
YOUTH AND SPORTS