EuroAsiaSPI^2 Blue Book Series

Selected Papers

Ed. by EuroAsiaSPI^2 (www.euroasiaspi.net) / EuroSPI^2 (www.eurospi.net) editorial board, editorial board, c/o ISCN GesmbH.

Selected Papers
24th EuroAsiaSPI^2 Conference

6.-8. September 2017
VŠB - Technical University of Ostrava, Ostrava, Czech Republic

www.eurospi.net
www.euroasiaspi.net

IMPRINT:

Selected Papers
24th EuroAsiaSPI Conference

6.-8. September 2017
VŠB - Technical University of Ostrava, Ostrava, Czech Republic

ISBN: 978-3-9504505-0-7

ed. by EuroSPI^2 (www.eurospi.net), EuroAsiaSPI^2 (www.euroasiaspi.net) editorial board, c/o ISCN Gesmbh., Dr. Richard Messnarz, Schieszstattgasse 4/2, 8010 Graz, Austria
Published, Sept. 2017
printed by Dorrong, Graz, Austria 2017
Series formerly published by Delta, Denmark, and Whitebox Denmark

EuroAsiaSPI² 2017 – Selected Papers, the *Blue Book*

EuroSPI Proceedings - A Collection of Books and Journals

The selected papers in the Blue Book are only a part of the EuroAsiaSPI^2 proceedings.

The proceedings comprise the SPRINGER CCIS 748 book which includes all research papers and all experience papers which were accepted and were available at the time of the SPRINGER book design.

Springer

The *Blue Book* contains papers which will be invited to be further extended and forwarded for further review and acceptance by the Wiley Journal of Software: Evolution and Process. The acceptance is managed by an editorial board.

EuroAsiaSPI^2 2017
European & Asian Systems Software & Service
Process & Product Improvement & Innovation

Selected Papers

24th EuroAsiaSPI^2 Conference

6. - 8. September 2017 |
VŠB - Technical University of Ostrava | Ostrava |
Czech Republic |
www.eurospi.net |

And the proceedings comprise an annual EuroSPI volume in the Wiley Journal of Software: Evolution and Process with 10 selected papers representing experience reports or new applied research in SPI.

WILEY

In the years 2015 and 2016 we also published with the SQP/ASQ SW Quality Professional journal.

In 2017 some papers were promoted to an IEEE SW magazine, Dr Miklos Biro being one of the editors of that specific volume.

EuroSPI^2 & EuroAsiaSPI^2 Blue Book Series

The *Blue Book* is published with an ISBN number which is maintained by the EuroSPI^2 / EuroAsiaSPI^2 conference series.

ISBN 978-3-9504505-0-7

Acknowledgements

Some contributions published in this book have been funded with support from the European Commission. European projects (supporting ECQA and EuroSPI) contributed to this book including AQU (Automotive Quality Universe), and InnoTEACH (LET'S BE INNOVATIVE! Development of Creativity, Innovation and Entrepreneurship), and EMVOI (ISO 17024 Certification for EU Project Managers).

In this case the publications reflect the views only of the author(s), and the Commission cannot be held responsible for any use, which may be made of the information contained therein.

EuroSPI Committees Strategy

EuroSPI has updated its board structure starting from 2017 onwards. To address the scientific recognition by SPRINGER (annual book series since 2003), and Wiley (journal series since 2004), representatives from a set of leading universities and research networks have been established as a conference board. They also act as main editors for the various books and EU initiatives.

To address the involvement of leading industry we have extended the workshop community approach to give leadership to industry in special topics for which there are workshops around the conference. For instance, experts from Volkswagen, Continental, Robert BOSCH, SQS, Japanese Union of Engineers, etc. are leaders of workshop communities.

EuroAsiaSPI² 2017 General Chairs

General Chair & Workshop Chair
Richard Messnarz, ISCN, Austria
Vice President of the ECQA, www.ecqa.org – European Certification and Qualification Association

General Co-Chair
Micheal Mac an Airchinnigh, ISCN, Contact Point for Ireland

Conference Board

Rory O'Connor, Dublin City University, Ireland

Miklós Biró, Software Competence Center Hagenberg GmbH (SCCH) and Johannes Kepler University, Linz, Austria

Ricardo Colomo-Palacios, Ostfold University, Norway

Michael Reiner, IMC FH Krems, University of Applied Sciences, Austria, President of the ECQA, www.ecqa.org – European Certification and Qualification Association

Gabriele Sauberer, TermNet, Austria
Vice President of the ECQA www.ecqa.org – European Certification and Qualification Association

Christian Kreiner, Graz University of Technology, Austria

Workshop Community Chairs

WS 1: Gamification and Persuasive Games for Software Process Improvement, Information Technology, and Innovation Management

Rory O'Connor, Dublin City University, Ireland

Murat Yilmaz, Cankaya University, Turkey

WS 2: SPI in Industry 4.0 – The Digitalization of Design and Manufacturing

Andreas Riel, Grenoble Institute of Technology, France
Vice President of the ECQA www.ecqa.org – European Certification and Qualification Association

Michael Reiner, IMC FH Krems, University of Applied Sciences, Austria, President of the ECQA, www.ecqa.org – European Certification and Qualification Association

WS 3: Best Practices in Implementing Traceability

Bernhard Sechser, Methodpark, Germany

Rainer Dreves, Continental, Germany

WS 4: Good and Bad Practices in Improvement

Eva Breske, Bosch Engineering GmbH, Germany

Tomas Schweigert, SQS, Germany

WS 5: Best Practices in Design of Systems applying Functional Safety, Cybersecurity, and how much Agile is Possible (with examples from Automotive Industry, Medical Device Industry)

Alexander Much, Elektrobit/Continental, Germany

Jenny Gorner, KnowIt, Sweden

Miklós Biró, Software Competence Center Hagenberg GmbH (SCCH) and Johannes Kepler University, Linz, Austria

Richard Messnarz, ISCN, Austria/Ireland

WS 6: Experiences with Agile and Lean

Alexander Poth, VW Wolfsburg, Germany

Susumu Sasabe, JUSE, Japan

Antonia Mas, University of the Balearic Islands (UIB),Spain

WS 7: Standards and Assessment Models

Gerhard Griessnig, AVL, Austria

Klaudia Dussa-Zieger, imbus AG, Germany

Marion Lepmets, SoftComply, Estonia

Timo Varkoi, Fisma ry, Finland

WS 8: Team Skills and Diversity Strategies Empowering Innovation and Improvement

Gabriele Sauberer, TermNet, Austria
Vice President of the ECQA www.ecqa.org – European Certification and Qualification Association

Mirna Munoz, University of Zacatecas, Mexico

Chairs *Honoris Causa*

The following persons have helped to form EuroSPI more than 20 years ago and have an advisory role to the chair.

Jørn Johanson, Whitebox, Denmark

Morten Korsaa, Whitebox, Denmark

Risto Nevalainen, FiSMA, Finland

Organising Chairs

Organising Chair
Richard Messnarz, ISCN, Austria

Organising Local Chair 2017

Svatopluk Stolfa, VSB Ostrava, Czech Republic

Organising Local Chair 2017

Jakub Stolfa, VSB Ostrava, Czech Republic

EuroAsiaSPI² 2017 Programme Committee Members

EuroSPI² 2017 Scientific Programme Committee

Biro Miklos	John von Neumann Computer Society	HUNGARY
Calvo-Manzano Jose A.	Politechnic University of Madrid (UPM)	SPAIN
Clarke Paul	Dublin City University	IRELAND
Colomo Palacios Ricardo	Ostfold University College	NORWAY
Dalcher Darren	Hertfordshire Business School	UK
Draghici Anca	Politechnic University of Timisoara	ROMANIA
Georgiadou Elli	-	UK
Kreiner Christian	University of Technology Graz	AUSTRIA
Kuvaja Pasi	University of Oulu	FINLAND
Landes Dieter	University of Coburg	GERMANY
Mäkinen Timo	Tampere University of Technology	FINLAND
Marcin Wolski	University of Poznan	Poland
Martins Paula	University of the Algarve	PORTUGAL
Mas Antonia	University of the Balearic Islands, UIB	SPAIN
Mc Caffery Fergal	Dundalk Institute of Technology	IRELAND
Mesquida Calafat Antoni Lluís	University of the Balearic Islands, UIB	SPAIN
Munoz Mirna	CIMAT- Unidad Zacatecas	MEXICO
O'Connor Rory	Dublin City University	IRELAND
Papatheocharous Efi	Research Institutes of Sweden RISE ICT/SICS	SWEDEN
Phalp Keith	Bournemouth University	UK
Reiner Michael	University of Applied Sciences Krems	AUSTRIA
Riel Andreas	Grenoble INP	FRANCE
Rodic Miran	University of Maribor	SLOVENIA
San Feliu Tomas	Politechnic University of Madrid (UPM)	SPAIN
Siakas Kerstin	Thessaloniki Institute of Technology	GREECE
Stolfa Jakub	VSB Ostrava	CZECH REPUBLIC
Stolfa Svatopluk	VSB Ostrava	CZECH REPUBLIC
Winkler Dietmar	University of Technology Vienna	AUSTRIA
Yilmaz Murat	Çankaya University	TURKEY

EuroAsiaSPI² 2017 Industrial Programme Committee

Balstrup Bo	InnospeXion ApS	DENMARK
Barafort Beatrix	Luxembourg Institute of Science and Technology (LIST)	LUXEMBOURG
Breske Eva	Bosch Engineering GmbH	GERMANY
Daughtrey Taz	American Society for Quality	USA
Dreves Rainer	Continental Corporation	GERMANY
Dussa-Zieger Klaudia	imbus AG	GERMANY
Ekert Damjan	ISCN GesmbH (Slovenia)	SLOVENIA
Fazal-Baqaie, Masud	CQM S&N INVENT	GERMANY
Fehrer Detlef	SICK AG	GERMANY
Gorner Jenny	Knowit	SWEDEN
Griessnig Gerhard	AVL LIST GMBH	AUSTRIA
Hallikas Jarmo	Falconleader	FINLAND
Ito Masao	Nil Software Corp.	JAPAN
Johansen Jorn	Whitebox	DENMARK
Karner Christoph	KTM Motorsport	AUSTRIA
Kaynak Onur	INNOVA	TURKEY
Kemaneci Kerem	TSE	TURKEY
Larrucea Uriarte Xabier	Tecnalia	SPAIN
Lepmets Marion	SOFTCOMPLY	IRELAND
Mac an Airchinnigh Micheal	ISCN GesmbH (Ireland)	IRELAND
Mashkoor Atif	Software Competence Center Hagenberg	AUSTRIA
Mayer Nicolas	Luxembourg Institute of Science and Technology (LIST)	LUXEMBOURG
Morgenstern Jens	-	GERMANY
Much Alexander	Elektrobit Automotive GmbH	GERMANY
Nevalainen Risto	Falconleader	FINLAND
Norimatsu So	JASPIC	JAPAN
Poth Alexander	Volkswagen AG	GERMANY
Renault Samuel	Luxembourg Institute of Science and Technology	LUXEMBOURG
Richard Messnarz	ISCN GesmbH (Austria)	AUSTRIA
Rozman Tomislav	BICERO	SLOVENIA
Sasabe Susumu	JUSE	JAPAN
Sauberer Gabriele	TermNet	AUSTRIA
Schweigert Tomas	SQS	GERMANY
Sechser Bernhard	Method Park Consulting GmbH	GERMANY
Soren Lyngso	LYNGSO Informatique Management Consulting	LUXEMBOURG
Spork Gunther	Magna Powertrain	AUSTRIA

Stefanova Pavlova Maria	CITT Global	BULGARIA
Stephane Jacquemart	EfCoCert	SWITZERLAND
Varkoi Timo	SPINET	FINLAND
von Bronk Peter	PB BestPractice	GERMANY
Wegner Thomas	ZF Engineering Plzeň s.r.o.	CZECH REPUBLIC
Witzgall Peter	PI.com	GERMANY

Welcome by the Local Organizers

Svatopluk Stolfa,
VSB TU Ostrava

Jakub Stolfa,
VSB TU Ostrava

Welcome to the 24th EuroSPI^2 Conference in Ostrava, Czech Republic

VSB – Technical University of Ostrava was founded in 1849, and has since grown into a modern institution of higher learning, offering the highest levels of education in technical and economic branches of study, based on the interconnection of science, research, education, and the creative activity that binds and enhances them.

Ostrava has long been a hub of major industry in central Europe, and study and research at VŠB-TUO is informed by historically close ties with major international companies, as well as by joint research and mobility programs with university partners the world over.

VŠB-TUO is the fourth largest university in the Czech Republic with over 20,000 students studying in bachelor's, master's and doctoral degree programs in seven faculties and two all-University study programs. VŠB-TUO has more than 2,500 employees. In November 2011 VŠB-TUO was awarded the prestigious ECTS Label, a mark of the quality of implementation of the credit system in bachelor and master study programs according to European standards. This label ensures that our administration of international students has undergone rigorous examination by an agency of the European Commission in order to receive this Label.

The University cooperates with educational and research institutions worldwide. From joint research programs with universities in the U.S., to cooperative degree and exchange programs in Europe, Japan, China, and beyond, VŠB-TUO holds international education as a priority which diversifies and strengthens not only our student body but the University as a whole.

VŠB-TUO is a public institution of higher education which provides tertiary education in technical and economic sciences. We prepare graduates for the future in a rapidly changing world. Our commitment is to implement education programs across different fields, using the research and development potential of the University. VŠB-TUO has more than one hundred accredited educational programs.

Research and Development connected to education are integral to the activities at VŠB-TUO. Our focus on applied research and close cooperation with industry informs the teaching activities at the University, ensuring relevance in a dynamic international scientific environment. T

VŠB-TUO is the project leader of the EU project AQU (Automotive Quality Universities, 2015-1-CZ01-KA203-013986, 2015- 2017) where a European partnership applied the AQUA (Knowledge Alliance for Quality in Automotive) concept with universities in Austria, Germany, France, and Czech Republic who educate people that will work in Automotive industry.

VŠB-TUO acts as the host of the 24th EuroSPI^2 Conference in Ostrava, Czech Republic. We are welcoming all participants to the Moravian-Silesian region.

Contact: Svatopluk Stolfa, e-mail: svatopluk.stolfa@scoveco.com, Jakub Stolfa, e-mail: jakub.stolfa@scoveco.com.

Welcome Address by the EuroSPI² General Chair

Richard Messnarz

ISCN, Austria/Ireland

EuroSPI is an initiative with the following major action lines http://www.eurospi.net:

- Establishing an annual EuroSPI conference supported by software process improvement networks from different EU countries.
- Establishing a social media strategy with groups in LinkedIn, Facebook, Twitter and online statements an, speeches and key notes on YouTube, and a set of proceedings and recommended books.
- Establishing an effective team of national representatives (from each EU- country) growing step by step into more countries of Europe.
- Establishing a European Qualification Framework for a pool of professions related with SPI and management. This is supported by European certificates and examination systems.

EuroSPI has established a joint newsletter with the European Certification and Qualification Association (www.eurospi.net, in the menu "About EuroAsiaSPI"), the SPI Manifesto (SPI = Systems, Software and Services Process Improvement), a set of social media groups including a selection of presentations and key notes freely available on YouTube, and access to job role based qualification through the European Certification and Qualification Association (www.ecqa.org).

A typical characterization of EuroSPI is reflected in a statement made by a company: "... the biggest value of EuroSPI lies in its function as a European knowledge and experience exchange mechanism for SPI and innovation."

Since its beginning in 1994 in Dublin, the EuroSPI initiative has outlined that there is not a single silver bullet with which to solve SPI issues, but that you need to understand a combination of different SPI methods and approaches to achieve concrete benefits. Therefore, each proceedings volume covers a variety of different topics, and at the conference we discuss potential synergies and the combined use of such methods and approaches.

Join the community of cross-company learning of good practices!

Contact: Richard Messnarz, ISCN GesmbH, Austria, e-mail: rmess@iscn.com

Welcome by the ECQA President

Michael Reiner

ECQA, Austria

The European Certification and Qualification Association (ECQA) is a not-for-profit association joining together institutions and several thousand professionals from all over Europe and the world. The association provides a world-wide unified certification schema for numerous professions. The same exam pool, exam rules and the same electronic exam system are used for certification exams in any participating country. It joins experts from the market and supports the definition and development of the knowledge required for job roles. ECQA defines and verifies quality criteria for Training organizations and trainers to ensure the same level of training all over the world.

Nowadays it is important that training courses are really recognised and attendees receive a certificate valid for all European countries. As a backbone of this initiative the EU supported the establishment of the ECQA almost 10 years ago.
The European Certification and Qualification Association (ECQA) is the result of a number of EU supported initiatives in the last ten years where in the European Union Life Long Learning Program different educational developments decided to follow a joint process for the certification of persons in the industry.

The overall objective of the project was to establish the ECQA which is supported by training organisations from European countries (currently organisations from 18 countries participate) developing and maintaining a set of quality criteria and common certification rules which are applied across the different European regions in the Life Long Learning scope in the IT and services, engineering, finance and manufacturing sectors.
This resulted in a pool of professions in which a high level of European comparability has been achieved by an Europe-wide agreed syllabus and skills set, an European test questions pool and European exam (computer automated by portals) systems, and a common set of certificate levels and a common process to issue certificates.

Through the ECQA it becomes possible to attend courses for a specific profession in one country and perform a Europe-wide agreed examination at the end of the course. The certificate will be recognized by European training organizations and institutions in 18 member countries by more than 60 ECQA members. With the help of Ambassadors the ECQA is also enhancing its activities by expanding to all over the world (e.g. USA, China, Thailand, India, Singapore, Japan etc.).

Michael Reiner, president of the ECQA and lecturer for Business Administration and E-Business Management at the IMC University of Applied Sciences Krems, has several years of experience in the field of IT, Microsoft Office, Microsoft NAP (ERP), Knowledge Management, Business Intelligence, Web 2.0, social networks and VR&AR. Moreover, Mr. Reiner coordinates and participate various EU projects. In the last nine years, ECQA has developed towards an international certifier issuing certificates and establishing partnerships in all European countries as well as in India, South America, China, Japan and Arabia. This expansion on the one hand enriches ECQA and its job roles with new views and different cultural aspects but also shows that there be the need of approaches for the solution of international certification schemas.

I wish you a good time at the EuroSPI² 2017 in Ostrava, a lot of interesting networking partners and exploratory meetings.

Contact: Michael Reiner, President of ECQA and Lecturer of IMC University of Applied Sciences, Austria, e-mail: ecqa_president@ecqa.org

Table of Contents

Workshop 8: Team Skills and Diversity Strategies

EuroAsiaSPI2 Blue Book Series

Mapping of Blue Book Papers onto Conference Sessions

Day	Time	Session	Paper
6.9.2017	09.00	WS6	Lean Layout Kaizen Case Study to Create One-Piece-Flow and Prepare for Pull Implementation in a Company Experimenting Lean Transformation
6.9.2017	10.00	WS7	Benefits of Defect Taxonomies and Validation of a new Defect Classification for Health Software
6.9.2017	11.30	WS7	A Proposed Model for Software Process Assessment and Improvement in the domain of Global Software Development
6.9.2017	14.00	WS8	Autonomous Vehicles - Social Impact
7.9.2017	12.00	WS2	An Approach for Data Security in the Era of Industry 4.0
7.9.2017	15.00	WS3	Best Practices of bi-lateral traceability implementation in Agile projects
8.9.2017	10.00	WS4	Formulation of Process Improvement Knowledge - 7 Components of a Good SPI Story
8.9.2017	11.30	WS5	Beware the IDES of March
8.9.2017	10.00	WS5	Extending Automotive SPICE 3.0 for the Use in ADAS and Future Self Driving Service Architectures

An Approach for Data Security in the Era of Industry 4.0 (extended abstract)

Masao Ito
NIL Software Corp. Tokyo, JAPAN
nil@nil.co.jp

1 My view of the industry 4.0

As for the Industry 4.0, in this paper, I assume that we are aiming for the distribution of the production bases. The web page of the industry 4.0 says: "Production and logistics processes are integrated intelligently across company boundaries to make manufacturing more efficient and flexible"[1]. This idea is a very attractive one, but we can quickly found out the issue of the security because we need the network to connect the factories.

Mainly we focus on the data, which is generated and maintained in the various places such as machines, the factories and the cloud system (figure 1). Of course, there are many points that we have to consider about security. But we first should focus on the concept design of the system; we can postpone the decision about the technical problems such as the level of cipher. In the first phase, we consider the level of security properties that the data must have. Because the security means that we keep assets from the threats. The data is one of the valuable assets.

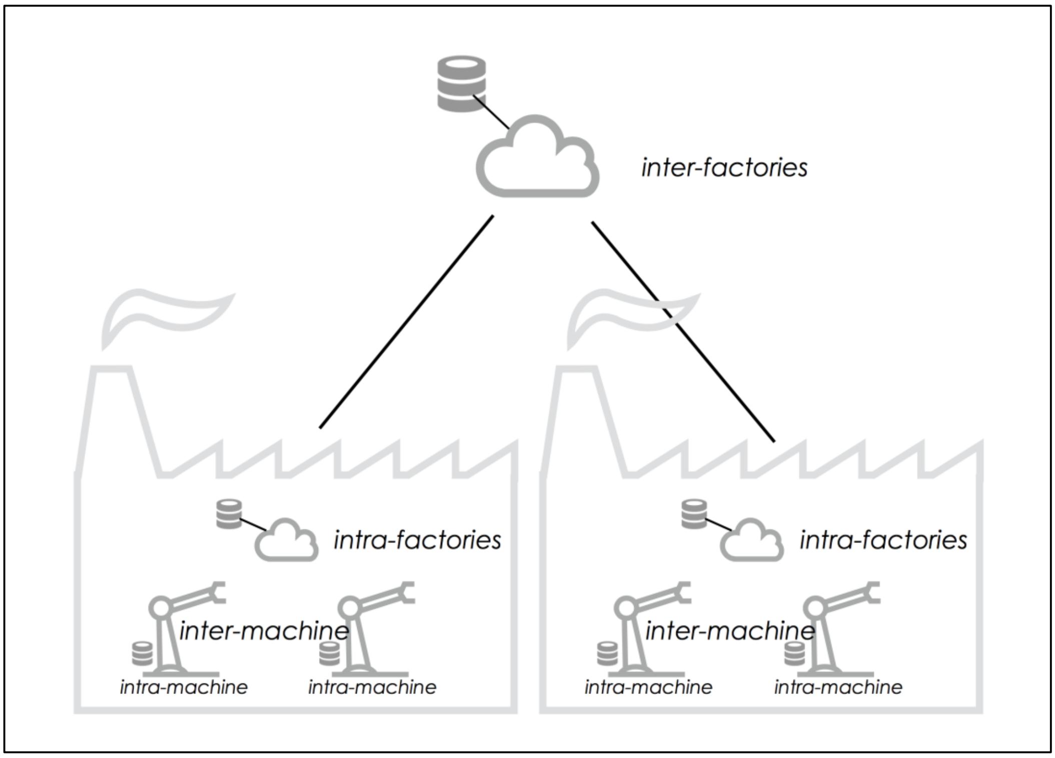


Fig. 1. The place of data in the industry 4.0 environment

Omnipresent Data

There are several types of data on which we have to focus [2, 3]; a) the core data by which we can produce the products and this data is stored in the database, b) the dynamic data that flows on the network, c) the infrastructure data that is the data for configure the machines.

We also consider the layers, typically like:

- Inter-factory level
- Intra-factory level
- Inter-machine level
- Intra-machine level

So, we have to check the 3x4 matrix to check the security violation.

Mainly, There are two causes of the security violation. The one is the alternation or deletion of data by who the malicious person or the organization, the second is the human error when setting or operating the system. In both cases, it is hard to protect systems from this violation. As for former, we have several evaluation mechanisms like the common criteria (CEM: Common Methodology for Information Technology Security Evaluation). But it doesn't provide the design process of the system or system of systems.

2 An Approach

I propose a simple approach that is just focusing on the data security. First, we identify the important data, and weight it from the viewpoint of keeping assets. Then we can find out the threats that we have to deal with. This approach is almost same as the previously proposed one [4].

I also provide the similarity and difference between the ISO 26262 functional safety approach and the data security approach.

3 References

1. http://www.plattform-i40.de/I40/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html (accessed 12/4/2017)
2. L. Harney, "Implementing the data safety guidance," 11th International Conference on System Safety and Cyber-Security (SSCS 2016), London, 2016, pp. 1-12.
3. SCSC, “Data Safety Guidance Version 2.0”, 2017.
4. Ito, M., Finding Threats with Hazards in the Concept Phase of Product Development. In Systems, Software and Services Process Improvement, Barafort, B.; O’Connor, R.; Poth, A.; Messnarz, R., Eds. Springer Berlin Heidelberg, Vol. 425, pp. 277-284, 2014

Best Practices of bi-lateral traceability implementation in Agile projects

Chandan Shivaramu
Tel: +91-9167-949923, chandan.shivaramu@here.com
HERE Solutions, Unit #2, NESCO IT Building, NESCO Complex, Next to Hub Mall, Goregaon East, Mumbai, India, 400063

Abstract

This paper aims to share the best practices to implement bi-directional traceability requirements in agile software projects that are need to be compliant with Automotive SPICE.

Keywords

Traceability, Bi-lateral traceability, Automotive SPICE

1 Introduction

Software (SW) projects in automotive industry usually required to go through Automotive SPICE (A-SPICE) certifications as required by the OEM's.
Bi-lateral traceability (BT) is one of the mandatory compliance area for the engineering processes (in A-SPICE terms for ENG.4-8 processes) to successfully achieve Capability Level (CL) 1. This is one area project teams have struggled to find solution in industries and it becomes highly complex if there are multiple development teams involved in the project.
In most of the Agile software projects practicing Scrum framework, teams use Atlassian ALM tool suite namely JIRA and Confluence. Please refer to [5] for the statistics about Scrum being the most widely used agile methodologies and JIRA being the most widely used Agile Management Tools.
The best practices shown in this paper are derived using these tools including their plug-ins (Thus the traceability documentation overheads usually required using Excel or legacy tool are avoided here thereby making of use of the tools the engineering teams comfortable with).

2 Overview

Traceability Best practices are divided into the following 5 areas of software development.

1. Product Requirements
2. Software Requirements
3. Software Design
4. Software Construction

5. Software Testing

3 Tools used

Tool Name	Usage
JIRA	Project management
Confluence	Documentation
Git	Version Control System
Gerrit	Code Review
Zephyr	Testing plug-in to JIRA
Requirements Yogi	Confluence plug-in to create wiki based documents with traceable links to JIRA tickets.
Gerrit Code Review	JIRA plug-in to link Gerrit code reviews to JIRA tickets
Zephyr for JIRA	Test Management JIRA plug-in
Jenkins Integration for JIRA	Visualization of Jenkins builds in JIRA

Fig. 1. Tool chain used to implement bilateral traceability

4 Best Practices

4.1 Product Requirements

Product requirements are captured in confluence as wiki pages. Each unique requirement is identified using confluence plug-in called <Requirement Yogi> RY which helps an entry into a searchable identifier that can be indexed anywhere in confluence and it can be linked to any JIRA ticket.

4.2 Software Requirements

Software Requirements are captured as EPIC's and user stories (basically JIRA tickets) in JIRA tool. EPIC and user story are natively linked in the tool.
JIRA offers support of linking any ticket to any other ticket from any JIRA project.
BT of SW requirements to Product requirements are met through Requirement Yogi linkage between Confluence and JIRA respectively.

4.3 Software Design

Work products related to Software design namely software architecture and software detailed design are written in confluence.

Architectural elements and detailed design components are referenced through <Requirement Yogi> plug-in so that they are linked together.
BT between software architecture and software requirements is through RY ID’s. Software detailed design can also be implemented through JIRA tasks and linked to Software Architectural design through RY links.

4.4 Software Construction

Implemented software is stored in Version Control System Git. Code Inspection/Review is done through the tool Gerrit.
Gerrit Code Review can be linked to a JIRA user story using a separate tab within the JIRA ticket. Through this link, we can establish BT of SW requirements to Software Units.
BT from SW units to SW detailed design is established through Gerrit to Confluence through RY.
BT from SW units to SW unit tests are established within Gerrit-Git as they are stored and referenced together.

4.5 Software Testing

Test cases are written for Software Integration Testing and Software Testing processes using JIRA plug-in called Zephyr. This tool allows to link test cases with JIRA tickets thereby establishing BT between SW requirements to Software Testing.

There are also Build workflow tools like Electric Commander and Jenkins that are highly compatible with JIRA and can be used to address BT.
JIRA plug-in for Jenkins integration provides a traceability between a JIRA user story and a Continuous Integration (CI) software build.

4.6 Mapping of Traceability tools to Software engineering processes

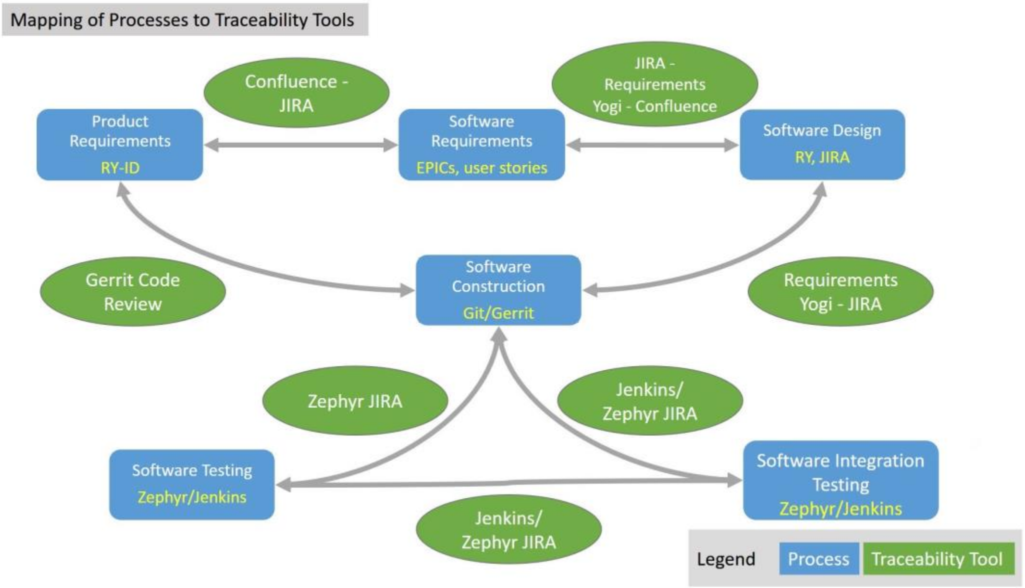

Mapping of Processes to Traceability Tools
Confluence - JIRA
JIRA - Requirements Yogi - Confluence
Product Requirements RY-ID
Software Requirements EPICs, user stories
Software Design RY, JIRA
Gerrit Code Review
Software Construction Git/Gerrit
Requirements Yogi - JIRA
Zephyr JIRA
Jenkins/ Zephyr JIRA
Software Testing Zephyr/Jenkins
Software Integration Testing Zephyr/Jenkins
Jenkins/ Zephyr JIRA
Legend
Process
Traceability Tool

Fig. 2. Traceability Mapping of software engineering processes to the tools

The above picture describes the mapping of software engineering processes with the traceability tools. Each process is implemented by the tool/s marked in yellow colored text.

5 *Summary and Conclusions*

Agile enabled organizations who are incorporating Scrum methodologies for their software development projects can easily demonstrate the traceability requirements of A-SPICE by adopting these best practices along with the recommended ALM tool chain.

If the Atlassian ALM tool chain (JIRA and Confluence) is already adopted by the organization, then the implementation of best practices will be much simpler.

The plug-ins to JIRA and Confluence mentioned in the paper are essential requirements to complete the traceability compliance required by the A-SPICE PAM version 2.5 standards.

The best practices described have been extensively used in many of our software projects which have been successfully certified for A-SPICE CL-3 for HIS scope of process set.

6 *References*

1. Requirements yogi Confluence plug-in, https://marketplace.atlassian.com/plugins

2. Gerrit Code Review for JIRA, https://marketplace.atlassian.com/plugins

3. Zephyr for JIRA, https://marketplace.atlassian.com/plugins

4. Jenkins Integration for JIRA, https://marketplace.atlassian.com/plugins

5. The 11th Annual State of Agile Report (2016) from VersionOne, http://stateofagile.versionone.com/

Formulation of process improvement knowledge
~ 7 components of a good PI story ~

So NORIMATSU, Kiyoshi ENDO, Makoto USUGI, Aiichiro NIWA, Eiwa KATAYAMA, Tomohiro HASHIMOTO, Koichi TANGE
Japan Software Process Improvement Consortium (JASPIC)
Toshima-ku, Tokyo, Japan
contact@jaspic.org

Abstract

The authors have been working within "Japan SPI Consortium" towards establishment of a knowledge structure for process improvement (PI). Our objective is to store useful knowledge, to provide mechanisms for their usage, and to encourage creation of new knowledge. During our efforts to extract, categorize and consolidate knowledge from the presentation materials at the conferences, we saw problems with respect to the coverage of knowledge expressed in the experiences. To solve this issue, we devised a knowledge model that consists of seven information elements as a representation, and then introduced a standard template to be used when submitting a proposal to the conference. As a result, statistically significant change in the coverage was observed, and the amount of information has increased for items such as causal analysis, verification and validation of process improvement. Positive feedbacks were obtained from proposal reviewers and conference participants for improved understandability. Percentage of successful stories has also increased among the presentations.

Keywords Process improvement knowledge, Formulation of knowledge, Coverage of knowledge, Standardization by template

1 Motivation for Formulation of Process Improvement Knowledge

1.1 Objectives for Japan SPI Consortium

Japan SPI Consortium (JASPIC), a non-profit organization established for collecting and disseminating “good practices” in Software Process Improvement efforts, have been organizing SPI conferences in Japan since 2003 [1]. Industrial experiences are presented along with keynote presentations, workshops, and tutorials. These presentations are publicly available for future usage.

To further develop systematic knowledge base of Process Improvement, the authors have formed a special interest group within JASPIC. We have analyzed these presentations to extract various forms of knowledge (e.g. keywords, concepts, principles, and good practices) so that it will support producing more successful stories in the community.

1.2 Challenges in Formulating Process Improvement Knowledge

Unlike in many other engineering domains, software development deals with human centric processes. It is quite rare for a specific process to be repeated under the exactly same condition. A “good practice” needs to be tailored with appropriate interpretation of the context.

Similarly, a “good Process Improvement practice” needs to be tailored. A specific solution used in one PI story may not reproduce the same outcome in another organization under different context. Reusability of PI knowledge (whether it is a “good practice in development” or a “good PI practice in PI activities”) is quite limited without contextual information.

This creates challenges in telling a “good” PI story from reusability perspective. First, it needs to communicate right amount of contextual information, but it may not be easy to do so for those who do not have adequate understanding of other organizations. Second, it is difficult to prove causality between the “solution” and the “outcome” in the story. One successful story under varying conditions may not be convincing in the future occurrence even in the same organization, much less in other organizations. As such, experience reports in SPI conferences tend to be anecdotal, or show inadequate analysis.

In 2012, we noticed that these challenges had become a barrier to formulate PI knowledge base from conference presentations. We first noticed that the information covered in these presentations is not complete enough to be transformed into a formal knowledge. We also noticed that we do not have a shared understanding in the community regarding the right contents to be included in a “good PI story”.

2 Components of Process Improvement Story

2.1 Basic Structure of Process Improvement Activity.

To clarify the essential components in a PI story, we began by establishing a basic structure as show in Figure 1.

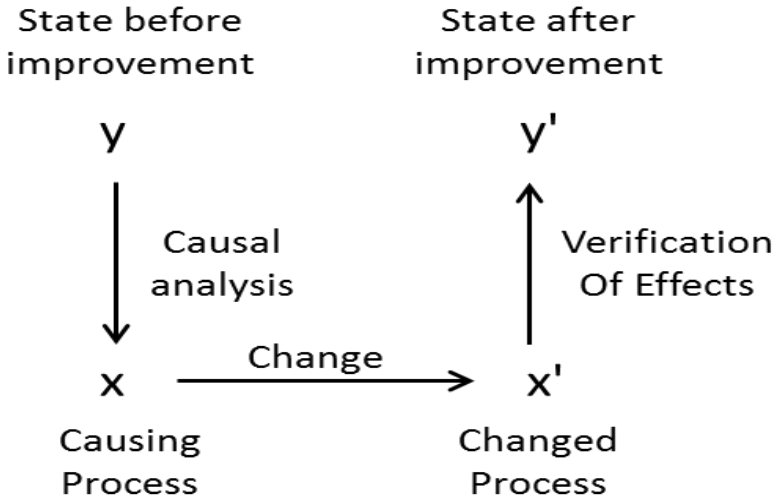


Fig. 1. Basic structure of process improvement activity

In Figure 1, the symbol y / y' denotes a state (an observed phenomenon) before / after improvement, and the symbol x / x' denotes a causing process before / after improvement. Process improvement, in a nutshell, is an effort to change an underlying process (x) to achieve a desired (improved) state (y'). It generally starts with an identification of state that requires an improvement, either in the form of current problem, and/or in the form of future desired result. Then it requires an identification of entities (e.g. process, resources, and inputs) that are causing the current situation. This typically requires a causal analysis or some form of hypothesis obtained from external knowledge. Changing a process typically requires major efforts and it is usually a primary focus of PI story. After the changed process has been performed, the result is analyzed to verify the impact of such a change.

Any PI story should include these elements to be considered "complete". Otherwise, it's a description of problems, hypothetical analyses, proposed solutions, incomplete efforts, or unproven experiments. Even in such an "incomplete" story, there can be many pieces of useful information. However, it becomes more useful when all these elements are provided in a consistent way so that it can be seen as a reusable package. A "good practice" can be established from such packages.

2.2 Additional Elements of Process Improvement Story

The basic package mentioned above provides a reusable set of information, especially under the same context. As mentioned in 1.2, however, for a larger community, additional context information is needed to understand the story and judge its applicability. Standard information needed to describe a context still needs to be clarified. According to the author's experiences, common information that audiences seem to want to know is for example application domain, organization's type, size, and project information. It also typically includes other background information that explains "why" the improvement effort started (e.g. purpose, or higher objectives).

Another useful piece of information to be communicated is a retrospective analysis or "validation" of a story. This would typically go back to the starting point of the story and see if the original intent or purpose of the improvement effort is satisfied. It also includes analyses such as cost-benefit calculation and identification of risks/issues and future improvement. This component of knowledge also communicates business values for wider audiences.

3 Promotion of Template for Process Improvement Story

3.1 Updating a Template for a Conference Presentation

To collect process improvement experiences that cover the essential components of PI story as discussed above, we decided to introduce a new form of template to be used at SPI Japan conference.

Traditionally, presenters at the conference submitted a presentation outline of about 2 pages in A4 (more than 1000 characters), and multiple reviewers evaluated them for utility and reliability. There was a brief template for this outline, which suggested that an outline includes "background, theme, contents (idea and original thought) and effect".

For 2013 conference, we expanded this template to cover the essential components plus more in-depth items. Below is an excerpt of a main part of the new template [2].
Main part of the new template (excerpt from “2013” version)
Background
Motive for the activity described in this presentation, original purpose and premise, etc.
State before improvement
Selected situation, problems and symptoms considered as improvement target.
And, the rationale of selection.
Causes that brought the state before improvement (i.e. causality)
Phenomenon and/or cause that created a state before improvement (e.g. some processes). There can be more than one phenomena or cause.
And, the method that revealed/selected/identified these phenomena and causes.
Content of changes and/or countermeasures
Change includes situations such as "Something is changed", "Something is abolished", and "A new thing is added".
And, the rationale of selection.
Implementation of changes and/or countermeasures
Activities performed to achieve the change or to implement the countermeasure.
And, any devised efforts, or issues that were encountered.
State after improvement and the effect of change
Changes that occurred after (5) “implementation of changes and/or countermeasures”.

- Changes of situation specified in (2) "state before improvement”, i.e. effect of change.
- And, verification of changes being not accidental. (if possible)

1. Validation of improvement activity

- Validity of the improvements, cost-effectiveness, remaining issues, secondary effect, after analyzing overall improvement activity.

3.2 Using and Continuously Improving a Template

Since the template was first released for 2013 conference, it has been recommended as a “standard” template. Presenters could also tailor it to add more chapters or modify as appropriate. They could also choose not to use it at all, but majority of the presenters used as it is or with minor modifications.

After the proposals were submitted, our group checked their contents to evaluate if they contain the intended components, and gave feedbacks to the presenters if necessary in addition to the comments from the official reviewers. We also asked the presenters to give us a feedback regarding the template. These comments helped us improve the template for the subsequent conferences. We now have updated it four times since the original release, and it has grown into a template and the guide with more explanatory statements, examples, and graphical representation of relationships among components as shown in Figure 2.

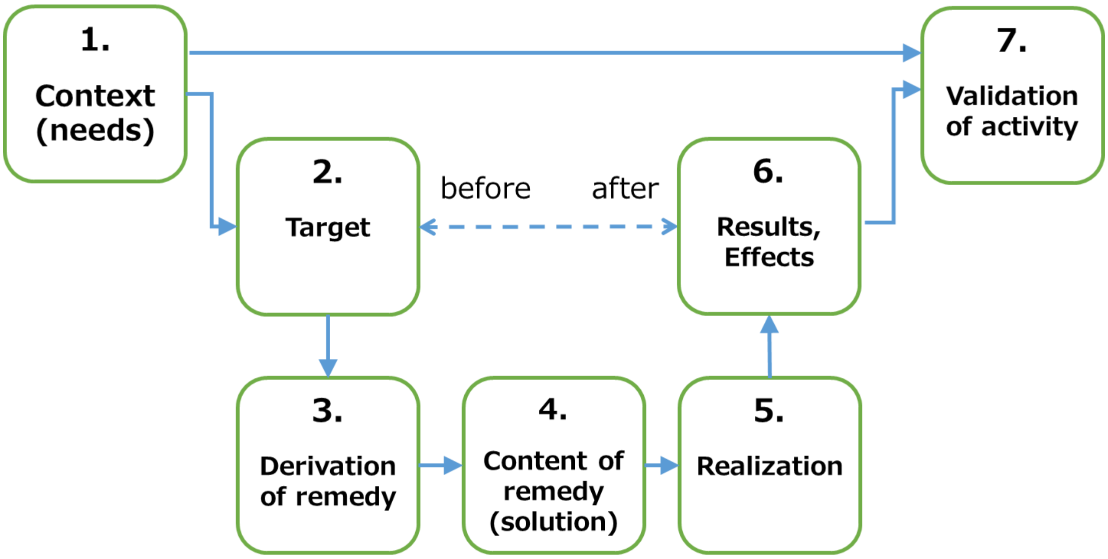


Fig. 2. Relationships among components

We have also conducted some workshops with consortium members and conference participants to discuss the usability of the template (and its underlying concept) for future improvement. This also helped them become familiar with the template so that it becomes easier for them to submit a proposal for the conference.

4 Effects by Introducing the Template

4.1 Initial Result in 2013

Evaluation Method:

To evaluate the effects of template introduction, we performed a comparative analysis of the coverage of presentation contents between those from 2011 (without the template) and those from 2013 (with the template).

The primary objective of our efforts was to improve the amount of information in the presentation, so we focused on the following two attributes for analysis:

(1) Completeness: whether the presentation includes the designated items in the template. There are 13 items (as bullets in the template) and each item is evaluated as "largely adequate" (1 point), "partially adequate" (0.5 point), or "inadequate" (0 point). Highest total score would be 13.

(2) Coverage: whether the presentation includes the basic components (chapters). If the first item (bullets) in each chapter is evaluated as "largely adequate", then the chapter is considered to be "covered" and given 1 point. Highest total score would be 7 for this attribute.

We randomly selected 25 presentations each from 2011 and 2013 conferences, and 5 people evaluated 5 cases each. To minimize variability due to subjective evaluation, sample cases were used to gauge the degree of variability, and adjust the evaluation process.

Evaluation Result:

The distribution of scores from 2011 conference is shown in Figure 3. The mean of Coverage score was 3.24 (out of 7), and the mean of Completeness score was 6.50 (out of 13), which means the presentations included only 50 % of what we consider a "complete story".

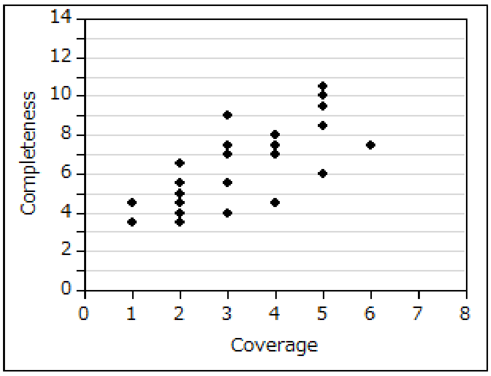


Fig. 3. Distribution of scores from 2011 conference

The distribution of scores from 2013 conference is shown in Figure 4. The mean of Coverage score was up to 4.32, and the mean of Completeness score was up to 7.80. The improvement ratio was 15% and 10% respectively.

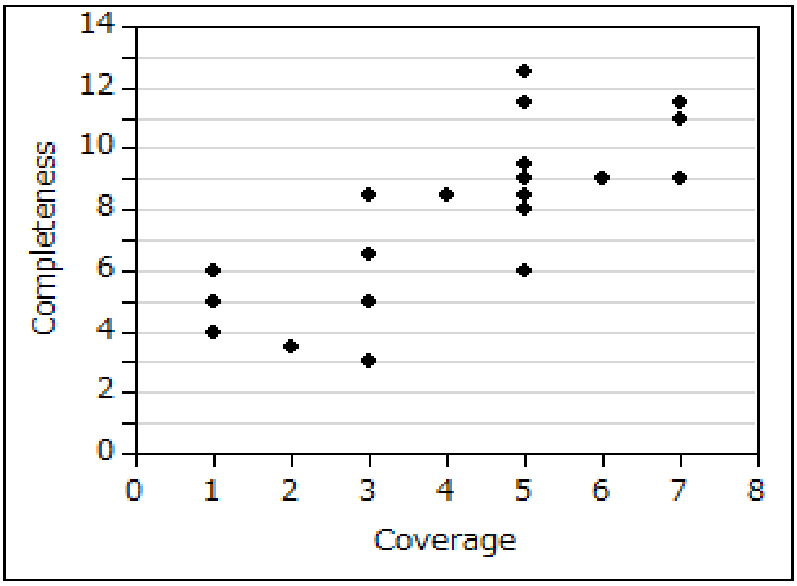


Fig. 4. Distribution of scores from 2013 conference

Statistical Analysis:

As we saw some improvements between 2011 and 2013, we further conducted statistical analysis to see if there is a statistical significance in the change.

Table 1 shows descriptive statistics of the attributes from 2011 and 2013, and Table 2 shows the result of significance tests.

Normality (by Shapiro – Wilk test) for Coverage score is rejected for 2013, possibly due to logical dependencies among the items, thus we looked at the result of Wilcoxon's test. The p is 0.0262 from the test, so we will reject the null hypothesis (i.e. suggesting significant change).

For Completeness score, normality and homogeneity of variance (by two-tailed F test) seems OK, so we can use the result of t-test. The p is about 0.05 so it's marginal, but not too bad to suggest a significant change in the result.

Table 1. Descriptive statistics of attributes (2011 and 2013)

	2011	2013
Coverage:		
Mean (%), and its 95% confidence interval	3.24(46%) [2.67-3.81]	4.32(62%) [3.55-5.09]
Standard deviation	1.39	1.86
Completeness:		
Mean (%), and its 95% confidence interval	6.50(50%) [5.65-7.34]	7.80(60%) [6.76-8.84]
Standard deviation	2.05	2.51

Table 2. Result of significance tests

	2011	2013
Coverage:		
Normality	p=0.068	p=0.0186

Homogeneity of variance	p=0.1602	
t-test	p=0.0246	
Welch’s test	p=0.0250	
Wilcoxon’s test	p=0.0262	
Completeness:		
Normality	p=0.3775	p=0.4875
Homogeneity of variance	p=0.3214	
t-test	p=0.0505	
Welch’s test	p=0.0507	
Wilcoxon’s test	p=0.0542	

4.2 Subsequent Results after 2013

Subsequent Evaluation Results:

As a result of initial analysis, we determined to continue to use the template in the 2014 conference. As mentioned in section 3.2, we continuously improved the template package and also performed supporting activities while monitoring each year’s presentations to see if we are getting good results.

Figures 5 shows evaluation results from subsequent conferences.

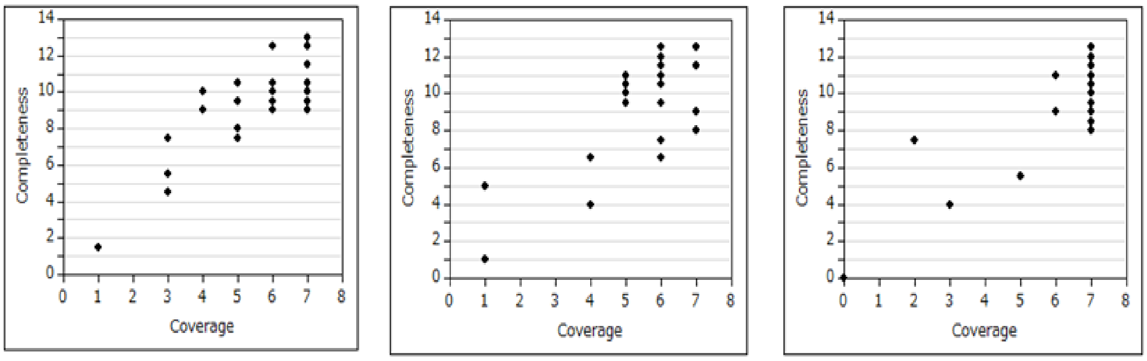


Fig. 5. Distribution of scores from 2014, 2015, and 2016 (from left to right)

Figure 6 shows the trend of Coverage and Completeness scores in the form of box-plot and 95% confidence interval of the average of each score. Coverage score shows steady improvement. Especially for 2016, the box plot is no longer a “box” as majority received 7 points. We consider that this attribute is no longer a major issue. Completeness score also shows improvement after 2013, but there’s a slight drop in 2016 (although not statistically significant). Average Completeness score is around 9.5-9.8 (out of 13) in the last three years, which is almost 50% improvement from 2011 conference, but we still have areas for improvement.

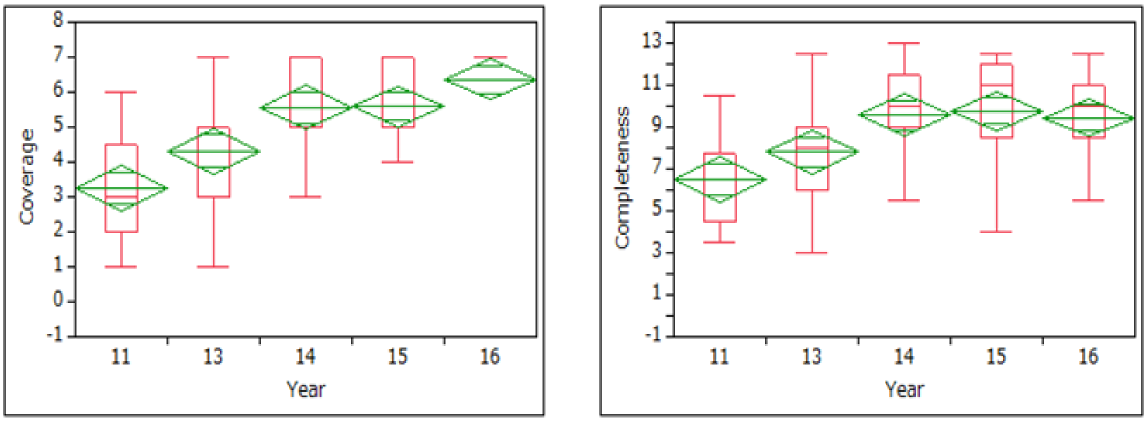


Fig. 6. Annual trend of scores from 2011 to 2016

Evaluation of Frequently Missing Items:

When we started this effort, there were a few frequently missing “items”, such as causal analysis of issues, (quantitative or statistical) verification of improvement results and validation of improvement activity. By introducing a template which is explicitly requesting these items, we expected that these items will not be missed too often.

Table 3 shows the scores of these specific items for 2011(before) and 2016(most recent). Two of these three items improved to a satisfactory level (above 90%), but the score for quantitative verification remains low. Considering the nature of the conference, it may be somewhat demanding to ask for this item, and we may not be able to expect this to be as high as other items.

Table 3. Comparison of scores for frequently missing items

Frequently Missing Item	Score in 2011	Score in 2016	Ratio (2016/2011)
causal analysis of issues	0.54	0.94	1.7
verification of results	0.06	0.30	5.0
validation of improvement activity	0.12	0.91	7.6

5 Quality of Process Improvement Knowledge

Although a definition of “Quality of PI knowledge” would require further discussion in the community, the authors believe that it includes at least applicability (or reusability) and effectiveness.

The efforts explained in this report showed improvements in the coverage of information, which will help increase the reusability of the PI stories reported in the community. At least, adequacy of information in these stories will help the understandability of such stories to determine their applicability. We have already heard positive (but yet qualitative) comments from reviewers and conference participants regarding this aspect.

Another aspect that might suggest the improvement in the quality of knowledge is the amount of “successful PI stories”. A successful PI story communicates an effective knowledge to the community by showing a positive outcome with verification and validation. We introduced a scoring method to evaluate the degree of verification (0-2 scale) and degree of validation (0-3 scale). The former score shows how the story is successful in terms of achieving the improvement target (e.g. solving the specified problems or achieving specified target), while the latter score shows how it is successful in terms of satisfying the needs (e.g. contributing to achieve a business value). Table 4 shows the comparison of average scores from 2011 and 2016. Again, we see a clear improvement in the scores, thus we conclude that our efforts have contributed to the improved quality of knowledge exchanged in the community.

Table 4. Comparison of scores for “successful stories”

	Score in 2011	Score in 2016	Ratio (2016/2011)
Score for verification	0.64	1.61	2.5
Score for validation	0.04	1.00	25.0
Total (verification + validation)	0.68	2.61	3.8

6 Conclusion

In order to collect “good process improvement stories” in the SPI conference in Japan, we formalized the structure of process improvement knowledge and standardized it as a template to be used in the conference proposal. As a result, the amount of information included in these PI stories increased steadily over the last four years. The quality of knowledge also improved as we saw significant growth in the scores of “successful stories”.

Address of Gratitude

This paper introduces activities performed by a special interest group for "software process improvement web of knowledge" in Japan SPI consortium (JASPIC).We are thankful to the JASPIC steering committee for supporting our activities. We’re also thankful to all the SPI JAPAN staff and presenters who provided cooperation and support for our efforts. We also thank those people who participated in the discussion to create this paper, especially Ms. Keiko Mizuta.

7 References

1. Ogasawara, Hideto: “Status of SPI Activities in Japanese Software – A view from JASPIC”, Industrial Proceedings, EuroSPI2013 (European Systems Software & Service Process Improvement & Innovation), pp.8.21 - 8.30.

2. Japan Software Process Improvement consortium: "SPI Japan 2013 presentation abstracts", Tokyo, 2013. http://www.jaspic.org/event/2013/SPIJapan/abstracts/abstracts.zip

“Beware the ides of March”– Future of (cyber)security testing

Paivi Brunou, Nixu, Finland
Päivi Brunou +358406601682
Paivi.brunou@nixu.com

Abstract. The Presentation key points
- Modus operandi for cybersecurity testing needs to change
- Controls are not enough!
- Left sift. Yes, start earlier and test incrementally
- How about the blue team?
- Bug bounties, crowdsourcing short term bliss or here to stay?

1 Motivation for Presentation

Organizations invest in defensive security measures, monitoring and (external) security team(s) to protect their business. Yet It takes on average 69 days to realize that your system has been compromised. In many cases this information is then received from 3rd parties like customers or governmental agenises.
“Beware the ides of March” the recommendation in Shakespeare’s Julius Cesar is both clear (you better watch out) and at the same time enigmatic. The problem is that the message was incomplete. As many companies traditionally focus on building controls (And yes, many cyber- attacks could be prevented by implementing basic controls) companies are not really prepared when the breach happens. This is why testing efforts need to be geared towards providing information for detection, recovery and remediation.

In the world of micro services systems like headless ecommerce are build more and more based on components and libraries. This means less written code and more integrations and API’s. These kinds of environments are tricky for traditional testing as the change can happen in multiple locations and high level of automation is often crucial. Like any other testing activities, security testing needs to leverage both static and dynamic testing and various methods throughout the whole development lifecycle.
Simply left sift. The regular Security assessment with production ready environment with production ready data just prior launch is merely providing you information. In addition, quality attributes like performance, usability and security are often creating overlapping and contradiction requirements.

A red teaming exercise is a simulation of a realistic threat agent targeting a specific organization. The attack is persistent and multiple attack avenues are tried to reach the end goal. The end goal is to obtain information that is commonly vital for the organization under attack. While red teaming has gained attention lately – how about the counterpart – Blue teams? How testing can support the combination of people, tools and processes work in practice to response to targeted attacks where goal is to obtain for example R&D trade secrets, finance, HR and other competitive information.

Crowdsourced security testing and bug bounties have gained attention in lately due to big bounties and media appeal. But are these longer term solutions or just for short fun ? Pro's and Con's, discussion and percolation on whether these are right for your test strategy.

1.1 Background

Engaged discussions with colleagues, QA enthusiasts and various experts over the year energize me. Having had the opportunity to speak in various seminars has always taught me something new. Am passionate about knowledge sharing and supporting #everydaylearning.

My heart simply beats for quality and lean methods. I also have some sense of humour and drink coffee generously, (milk no more sugar, thank you). I prefer adapting various quality methods for context-driven approach and get all excited about matching measurable quality attributes and business needs.
Currently in the realms of #Cybersecurity LinkedIn: https://www.linkedin.com/in/paivibrunou/

Experience as speaker
• Delivering various internal trainings
• Event: Prosessipäivät 2016, April Helsinki Finland Topic: What's for Lunch?
Reseptejä prosessien kehittämiseen (In Finnish about SPI)
• Event: Software quality days, 2015/01 Vienna Austria Topic: Making quality
visible - selecting the quality attributes that count (Quality)
• Event: Profes 2014/12 Helsinki, Finland Applying the LAPPI Technique in QA and
Testing (SPI)
• Topic: Tutorial: Practical Process Improvements – Event: Europe 2014/06,
Luxembourg Topic: Workshop - Measurement "Five essential moves for visible

Extending Automotive SPICE 3.0 for the Use in ADAS and Future Self Driving Service Architectures

Richard Messnarz, ISCN GesmbH, Austria. E-mail: rmess@iscn.com
Christian Kreiner, Graz University of Technology. E-mail: christian.kreiner@tugraz.at
Georg Macher, AVL List GmbH, Austria. E-mail: georg.macher@avl.com
Alastair Walker, Lorit Consultancy LTD, Scotland. E-mail: alastair.walker@lorit-consultancy.com

Abstract

The SOQRATES (www.soqrates.de) working party has been established in 2003 with the support of the Bavarian SW initiative. Major Automotive suppliers joined forces to exchange best practices in topics such as Automotive SPICE, functional safety, and cybersecurity.

The Research method of SOQRATES is to compare the best practices and in case a specific design pattern is accepted by all parties it is declared as a state of the art for the group.

Some of the results of the working party have been packaged into training courses.

E.g. in the EU project SafEUr (518632-LLP-1-2011-1-AT-LEONARDO-LMP, 2011- 2012) a European partnership with inputs from SOQRATES developed a skill set, training materials and best practices for ISO 26262 promoting best practice design strategies which were exchanged in the partnerships.

E.g. in the EU project AQUA (Knowledge Alliance for Quality in Automotive, EAC-2012-0635, 2013- 2014) a European partnership with inputs from SOQRATES developed a skill set, training materials and best practices for integrating Automotive SPICE, ISO 26262, and Six Sigma.

E.g. in the EU project AQU (Automotive Quality Universities, 2015-1-CZ01-KA203-013986, 2015- 2017) a European partnership with inputs from SOQRATES applied the AQUA concet with universities in Austria, Germany, France, and Czech Republic who educate people that will work in Automotive industry.

Also the working party elaborated integrated assessment models where the Automotive SPICE 3.0 has been merged with ISO 26262 (further safety related questions) and SAE J3061 (further cybersecurity questions).

This paper will look into the future of self-driving cars and discuss the design patterns which are currently analysed in the working party to support a vehicle in future self-driving infrastructure architectures and processes.

Keywords

Automotive SPICE, Functional Safety, cybersecurity, ISO 26262, SAE J3061, Service Architectures for Automotive

1 Introduction

ADAS stands for Autonomous Driving Assistance Systems and realizes functions that support the driver but still keep the driver in the flow. It is still expected that there is a driver with a driver license who is part of the control flow. From 2030 on the plans from OEMs are to produce self-driving cars where there are no drivers, the passenger is a person that is provided with a mobility service. The car itself must control the situation (supported by infrastructure) and also the insurance model will have been changed by then. Cars will have a black box that logs all vehicle data from all ECUs and insurance will go with the car and the component, and will not be on the driver as a person any more. In case of the steering example in this paper, the authors also outline the future of a self-driving scenario.

Automotive companies experience an exponential increase in functional development. Major car manufacturers develop vehicle functions which can be decomposed into features (functions) on ECU and supplier level. A real time communication (via a bus) of a set of ECUs then realizes the vehicle functions. ECUs have SW and usually control a mechatronic system.
Automotive projects need to implement standards which help to cope with this new complexity where more than 100 ECUs (Electronic Control Units) are networked by a bus system, and vehicle functions are implemented by a real time sequence of commands to these ECUs actuating several subsystems. In volume 17, Issue 3, June 15 of the Software Quality Professional magazine we discussed the implementation of Automotive SPICE and Functional Safety in an integrated approach [14].
In Software Quality Professional, American Society of Quality, Volume 18, Issue 4, September 2016 we discussed the extension of this integration to include the new cybersecurity standard SAE J3061 [13].
In the SAE Integrated Safety and Security Development in the Automotive Domain, Working Group 17AE-0252/2017-01-1661, SAE International, June 2017 publication we describe how the vehicle functions architecture will be extended by a cybersecurity architectural design to cover both, functional safety and cybersecurity at the same time [16].

In this paper we further extend the vehicle architecture to include interfaces with the service architecture which will be required for future self-driving scenarios. Self-driving car functions are becoming a competitive factor for manufacturers. However, these new systems will require an additional layer of service architecture which again will need assessments.

2 Current Status of Safety Application – ISO 26262

In [13] the ESCL (Electronic Steering Column Lock) system was used as an example to explain the steps to analyse the safety-critical item according to the ISO 26262, perform a hazard and risk analysis, apply decomposition and diagnostic coverage principles and come up with a system-, software- and hardware design that fulfils ASIL D criteria. Also the requirements and test traceability of Automotive SPICE was explained.
In this paper we apply the same analysis and design principles on a steering system.

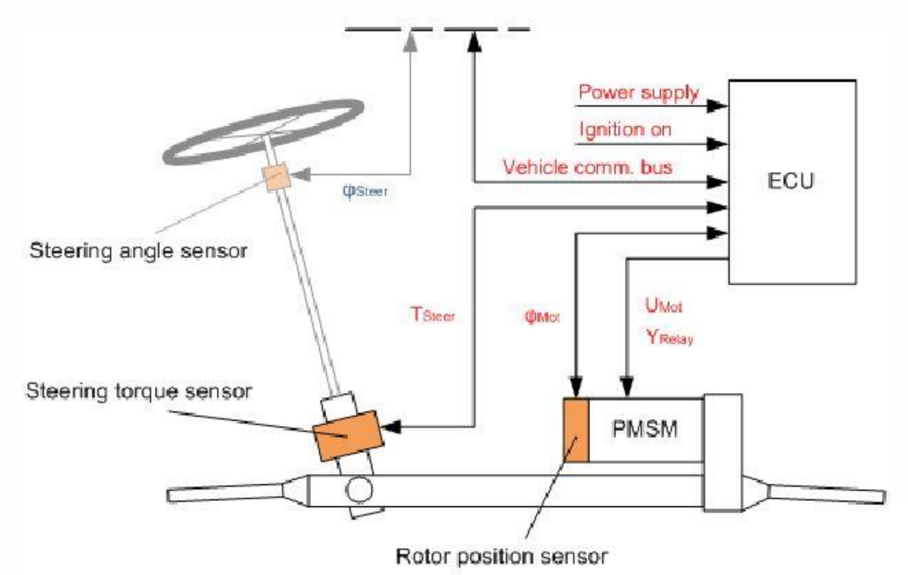
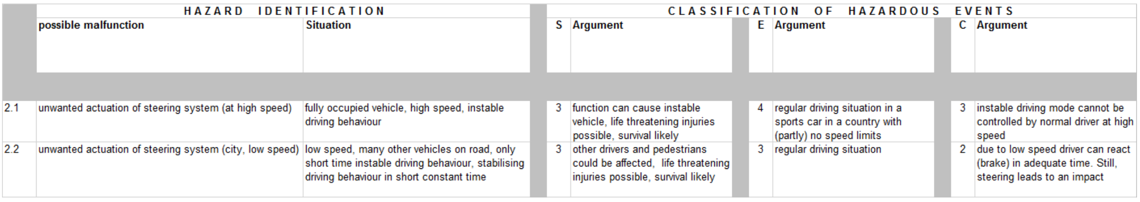


Figure 1: Example of a safety item definition (Electronic Steering System)

In the hazard and risk analysis and analysis of an item (a high level design with ECU, SW, electronic elements and their interfaces) ASIL (Automotive Safety Integrity Level) levels are assigned to hazardous events and safety goals are formulated. An item definition and analysis also requires a functional understanding of the item.
Example electronic steering system (based on the above Fig.1): The driver steers and the steering angle sensor is a separate ECU which puts the steering angle on the bus. The steering of the driver is measured by a steering angle sensor (integrated into the steering column) and the steering torque is an input to the ECU (Electronic Control Unit). The ECU controls an E-Motor to support the requested torque and measures the achieved angle position by a rotor position sensor (with a rotor angle, motor torque, and a calculated index position which determines the position of the steering rack).
The ISO 26262 safety analysis delivers ASIL ratings for different hazardous events. The Fig.2 shows the example rating one of the most hazardous events (ASIL-D). According to ISO 26262 there are tables which help to rate S (Severity) 0-3, E (Exposure) 0-4, C (Controllability) 0-3.



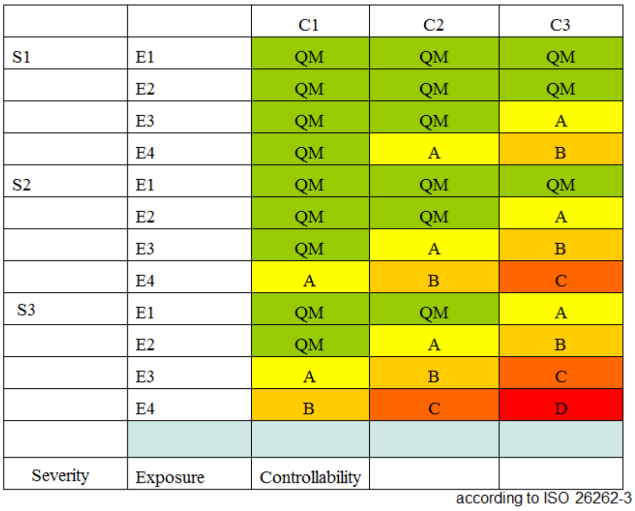
	HAZARD IDENTIFICATION			CLASSIFICATION OF HAZARDOUS EVENTS				
	possible malfunction	Situation	S	Argument	E	Argument	C	Argument
2.1	unwanted actuation of steering system (at high speed)	fully occupied vehicle, high speed, instable driving behaviour	3	function can cause instable vehicle, life threatening injuries possible, survival likely	4	regular driving situation in a sports car in a country with (partly) no speed limits	3	instable driving mode cannot be controlled by normal driver at high speed
2.2	unwanted actuation of steering system (city, low speed)	low speed, many other vehicles on road, only short time instable driving behaviour, stabilising driving behaviour in short constant time	3	other drivers and pedestrians could be affected, life threatening injuries possible, survival likely	3	regular driving situation	2	due to low speed driver can react (brake) in adequate time. Still, steering leads to an impact

Figure 2: Example Hazard and Risk Identification rating

The risk graph then translates the rating of S,E,C into an ASIL rating (see Fig.3).

Determination of ASIL

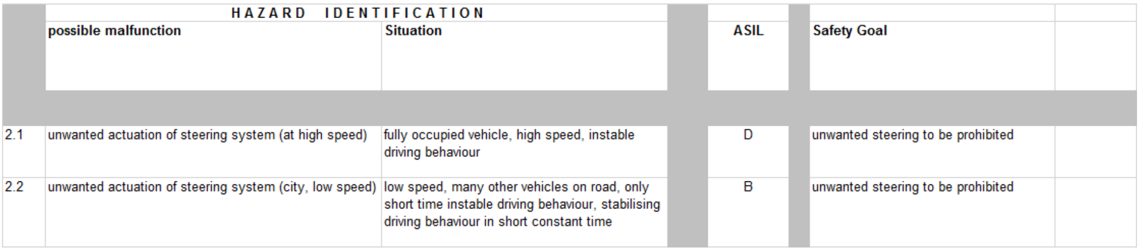
Note: QM requires a quality management system if at least one function is rated ASIL A or higher



		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D
Severity	Exposure	Controllability		

according to ISO 26262-3

Figure 3: Risk Graph According to ISO 26262



	HAZARD IDENTIFICATION				
	possible malfunction	Situation	ASIL	Safety Goal	
2.1	unwanted actuation of steering system (at high speed)	fully occupied vehicle, high speed, instable driving behaviour	D	unwanted steering to be prohibited	
2.2	unwanted actuation of steering system (city, low speed)	low speed, many other vehicles on road, only short time instable driving behaviour, stabilising driving behaviour in short constant time	B	unwanted steering to be prohibited	

Figure 4: ASIL rating for example in Figure 1

Faults in the hardware lead to errors which can cause failures on the system level. The system analysis identifies such faults and errors that can lead to the failures which creates the hazard of unwanted steering. Below are an example list of errors which can cause the ASIL-D classified hazard:

Hazard: The steering angle sensor delivers wrong input and self-steering is happening.

Hazard: The torque sensor is measured incorrectly and oversteering or understeering takes place.

Hazard: The steering angle data are sent wrongly on the bus (other devices like ESP are steering in different direction) leading to instable drive.

Hazard: The (**new with connected infrastructure**) requested steering angle from the service infrastructure is incorrect and an incorrect steering takes place.

In [13] the hazard and risk classification is explained with the ESCL example. Here we apply the same principle on an electric steering system. The H&R (Hazard and

Risk Analysis) delivered an ASIL D (highest rating of a safety classification) and a safety goal “No unwanted actuation of a steering system”.
When doing system analysis this safety goal needs to be broken down to system safety requirements. The safety experts and system analyst usually look at the potential faults that can lead to this failure (e.g. using the FMEA as a source) and define requirements to diagnose a d avoid these faults. Below are some examples:

Safety Requirement Example:

> Functional safety concept level: The steering angle is measured with ASIL-D quality.
>
> Technical Safety Concept level: The internal steering angle calculated from the rotor angle and index position is to be provided with ASIL-D quality.
> Remark: in most steering systems the supplier scope does not include the external steering angle sensor (comes from OEM), therefore the steering angle is calculated from rotor position sensors.
>
> Technical Safety Design level: The internal steering angle calculation is done with 2 rotor position sensors which are plausi-checked against each other. Each must fulfil the ASIL-B quality goals and the comparison is done with an ASIL-D rated ASIC. The ASIC delivers sin and cos angle information and index counter.
>
> > Remark: Here a decomposition took place where an ASIL D rated part (steering angle) was decomposed into 2 redundant and diverse ASIL-B rated elements. The decomposition approach is described in ISO 26262 [2,3,4,5]. Diversity must be proved by hardware (not having same fault behaviour) and algorithms (sin and cos function). The diversity aspect is only used for ASIL-D. The safety norm includes method tables [2,3,4,5] where such method approaches like diverse design are assigned to ASIL levels.
>
> Technical Software Requirement: Measuring every 1 ms the sin and cos and index counter and calculate a steering angle. Both steering angles must be same within an e.g. 5 degrees range (plausi-check). This comparison must be independently running and monitored.

In general the safe electric steering systems are limiting the torque so that not more torque than requested by the driver can be put onto the motor by the ECU. Therefore it is clear that the torque sensor is ASIL-D as well (Fig. 5, Fig.6).

Fig. 6 shows a decomposition example and the fact that a safety critical signal flow is designed which is being monitored by safety functions and also all hardware elements on this functional chain fulfil requested ASIL-defined FIT (Failure in time rates, part 5 ISO 26262:2011).
The requested torque is controlled by the ECU and measured by the rotor position sensors and effective torque measured must always stay smaller than the requested torque (see signal flow).

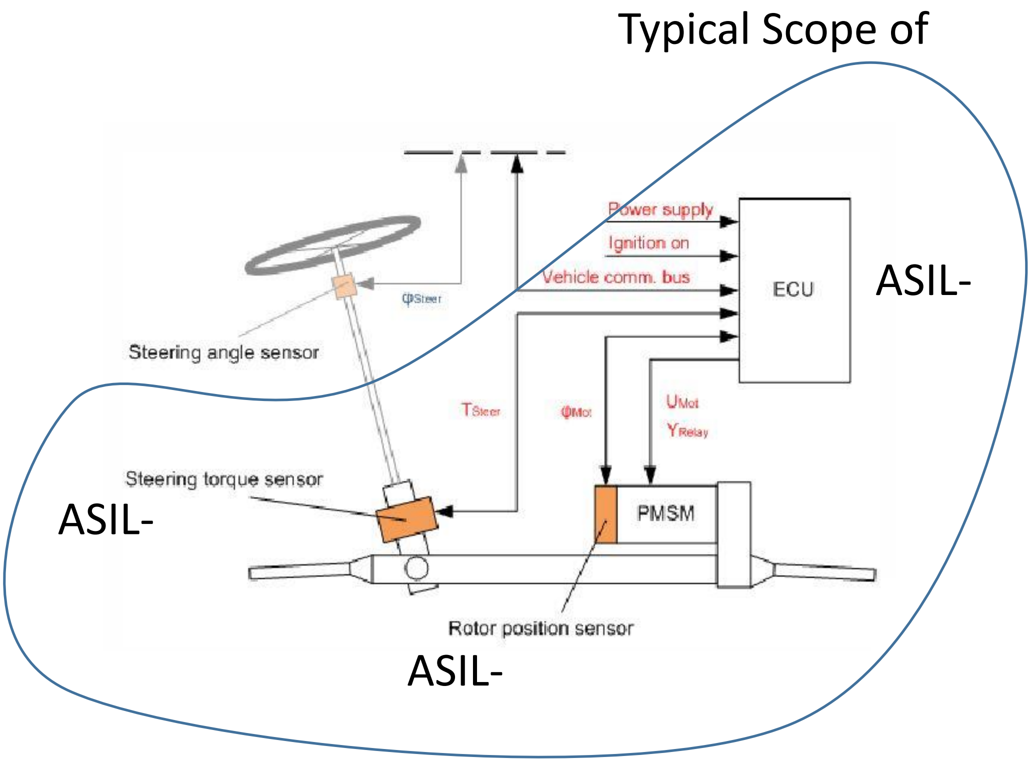


Figure 5: ASIL Assignment to Critical Signals / Elements based on safety Goal

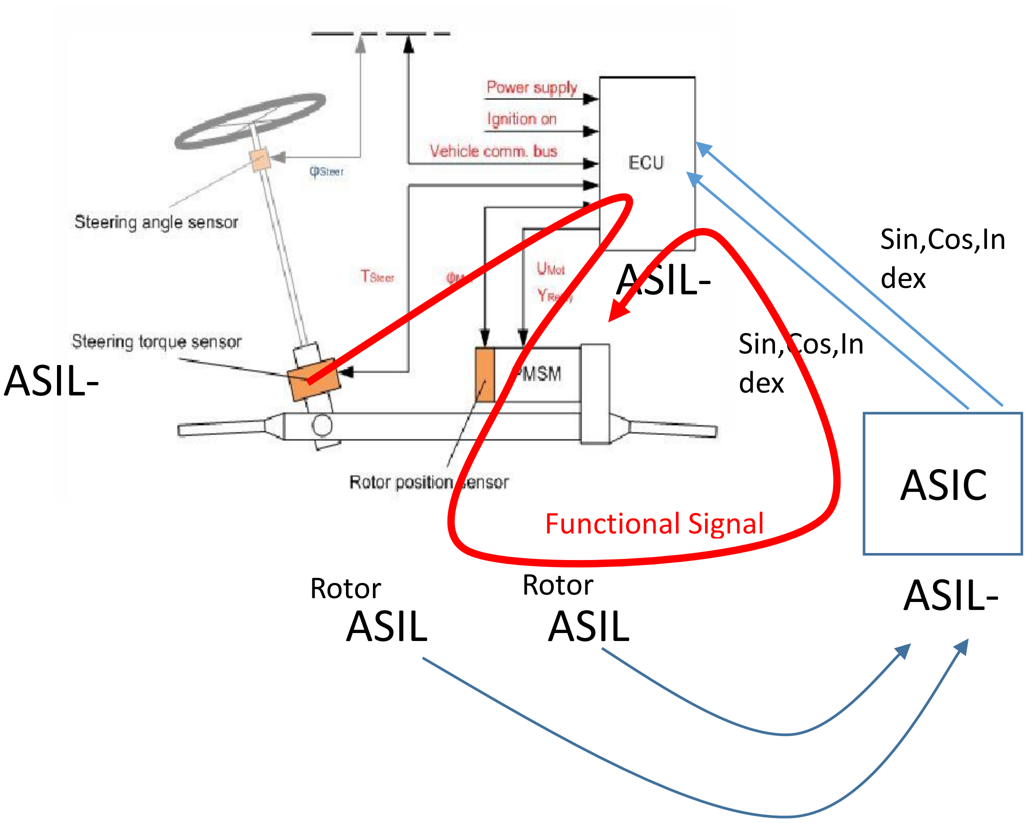


Figure 6: ASIL Decomposition, Redundancy, Diversity and Signal Flow

3 Future Self Driving Scenario

This approach will not work anymore in a full self-driving mode if the steering angle from the vehicle infrastructure (command from vehicle infrastructure) will be considered as the main input. In the next years still the driver has a steering wheel and can override the command by just producing a torque in the torque sensor in the steering column. However, when moving towards complete self-driving the commands from the vehicle infrastructure will take over.

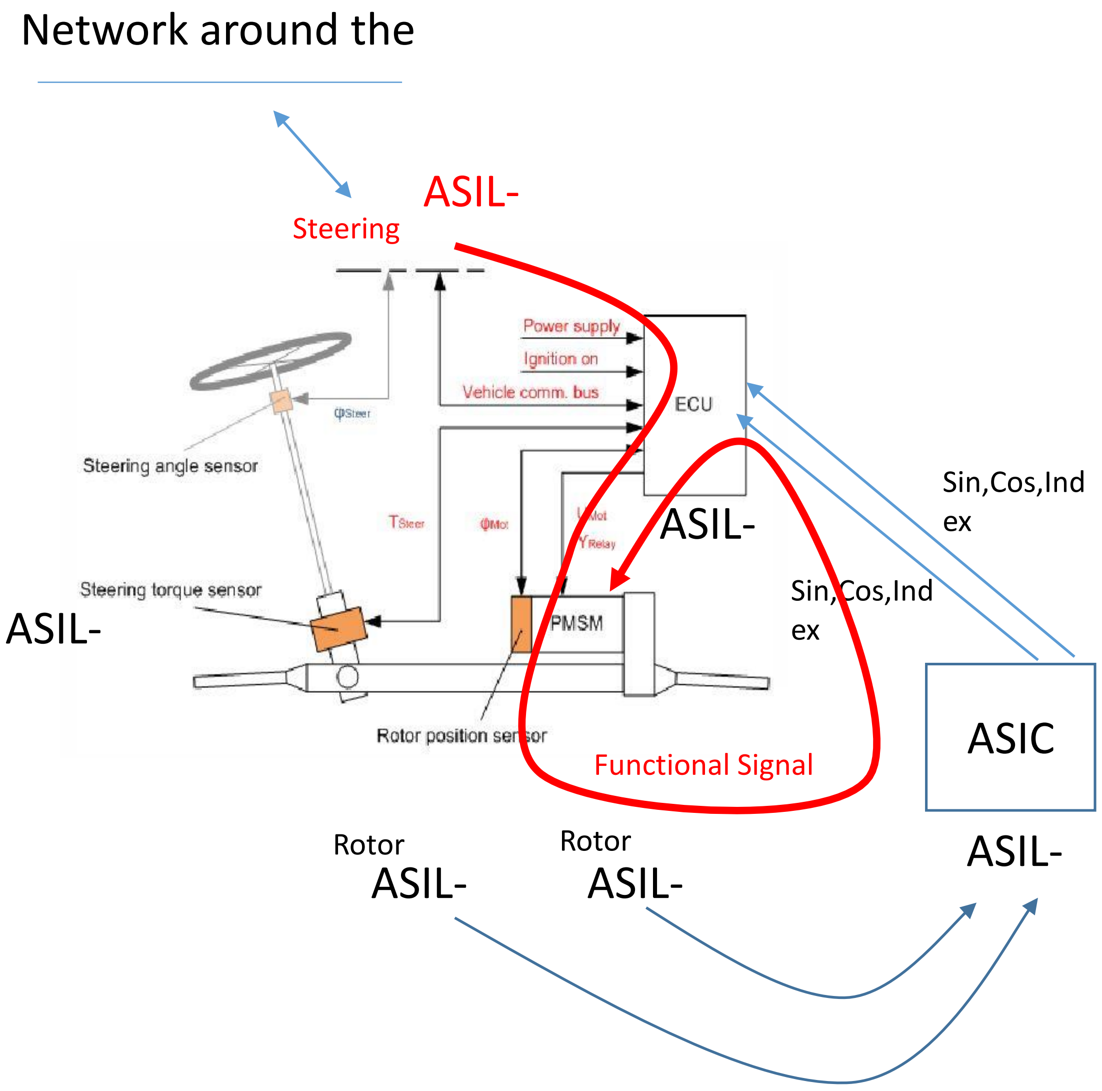


Figure 7: ADAS changing the safety critical signal flow

A command can come from the network (networked car) or from a central ECU in the car, and then even the safety goal will change.

> Safety Goal: Do not steer more than requested by the command. Commands then include a requested steering angle, this is translated in the ECU to a requested torque and the achieved angle position (internal steering angle) is then compared with the external requested steering angle.

Also the safe state will change, because in ADAS full implementation (latest from 2030) it is expected that we cannot give the control back to the driver any more. Therefore 6 to 12 phase e-motors are needed to continue driving and safe state would a kind of limp home mode to the garage with the car passenger (former a driver).

> Safety State: Using redundant and diverse motor concepts (6 phase, 12 phase) to allow a limp home mode to a garage with the driver.

Another bigger change is the distribution of ASIL values. While in solutions the typical scope of a supplier the external steering angle sensor was not in the scope and ASIL-D rating was on the internal steering angle provided as a message on the bus, in ADAS the functional signal flow will change as outlined in Fig.7.

4 Integrating Automotive SPICE, Functional Safety, Cybersecurity

In Automotive SPICE [1] - which most automotive companies integrated with functional safety in their engineering life cycle - the safety requirements are traced using the same concepts of traceability as for normal functional requirements [13], [14].

Figure 8 outlines the traceability between customer and system requirement level using a safety relevant example of requirements related to a steering angle command in ADAS. The dotted parts highlight the additional specifications which are influenced by the decomposition required for the ISO 26262 standard fulfilment.

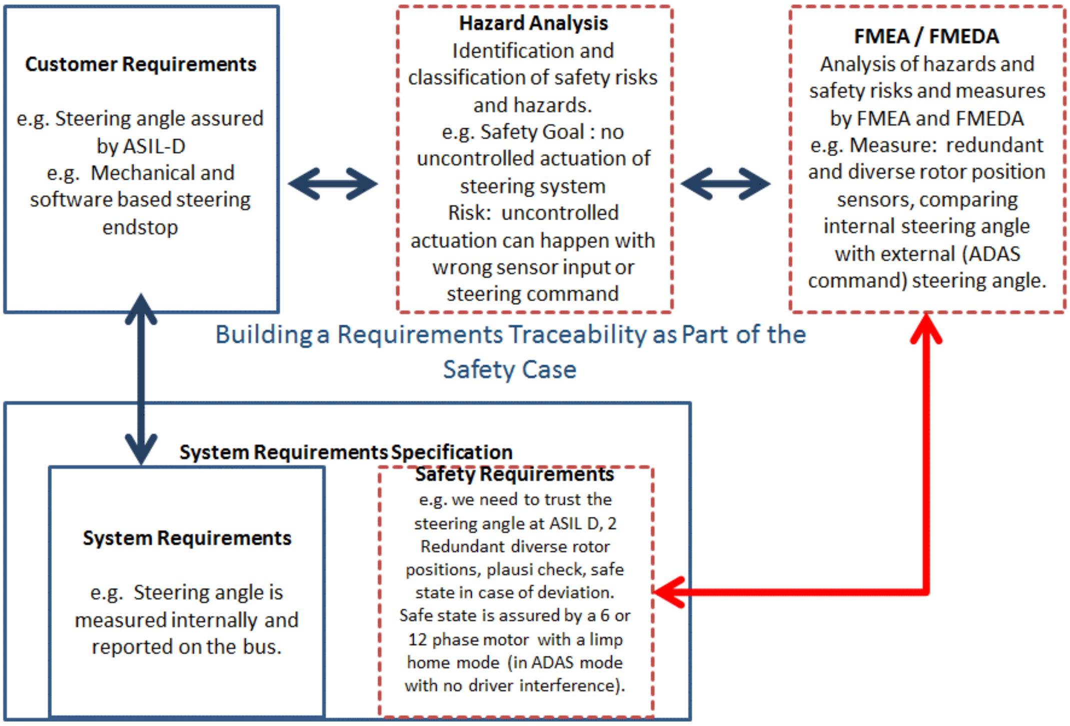
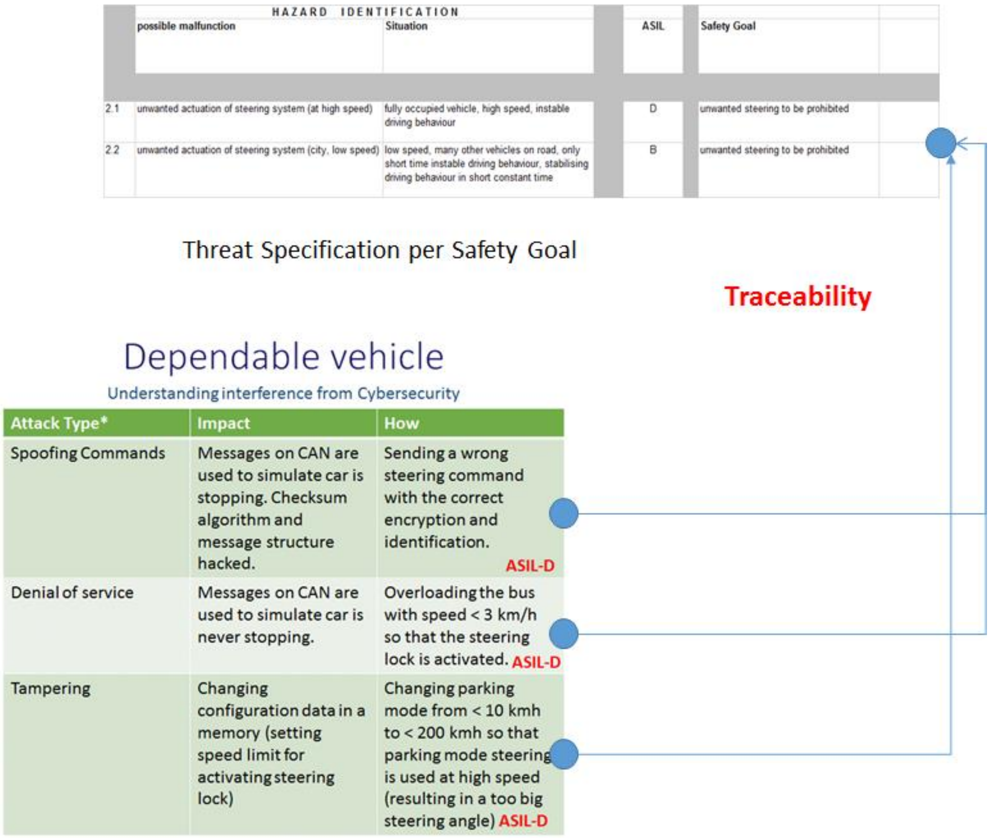

Customer Requirements
e.g. Steering angle assured by ASIL-D
e.g. Mechanical and software based steering endstop
Hazard Analysis
Identification and classification of safety risks and hazards.
e.g. Safety Goal : no uncontrolled actuation of steering system
Risk: uncontrolled actuation can happen with wrong sensor input or steering command
FMEA / FMEDA
Analysis of hazards and safety risks and measures by FMEA and FMEDA
e.g. Measure: redundant and diverse rotor position sensors, comparing internal steering angle with external (ADAS command) steering angle.
Building a Requirements Traceability as Part of the Safety Case
System Requirements Specification
System Requirements
e.g. Steering angle is measured internally and reported on the bus.
Safety Requirements
e.g. we need to trust the steering angle at ASIL D, 2 Redundant diverse rotor positions, plausi check, safe state in case of deviation.
Safe state is assured by a 6 or 12 phase motor with a limp home mode (in ADAS mode with no driver interference).

Figure 8: Traceability of ASPICE extended by Functional Safety Related Requirements

In cybersecurity the STRIDE [8] analysis of potential attacks is linked with safety goals and made traceable according to Automotive SPICE (Fig. 9) [14], [16].



HAZARD IDENTIFICATION

	possible malfunction	Situation	ASIL	Safety Goal
2.1	unwanted actuation of steering system (at high speed)	fully occupied vehicle, high speed, instable driving behaviour	D	unwanted steering to be prohibited
2.2	unwanted actuation of steering system (city, low speed)	low speed, many other vehicles on road, only short time instable driving behaviour, stabilising driving behaviour in short constant time	B	unwanted steering to be prohibited

Threat Specification per Safety Goal

Dependable vehicle

Understanding interference from Cybersecurity

Attack Type*	Impact	How
Spoofing Commands	Messages on CAN are used to simulate car is stopping. Checksum algorithm and message structure hacked.	Sending a wrong steering command with the correct encryption and identification. ASIL-D
Denial of service	Messages on CAN are used to simulate car is never stopping.	Overloading the bus with speed < 3 km/h so that the steering lock is activated. ASIL-D
Tampering	Changing configuration data in a memory (setting speed limit for activating steering lock)	Changing parking mode from < 10 kmh to < 200 kmh so that parking mode steering is used at high speed (resulting in a too big steering angle) ASIL-D

Figure 9: Traceability between safety goals and cybersecurity attack schema (Microsoft STRIDE concept)

And in cybersecurity [7,9,10,12,15,16] an additional view of a cybersecurity related defence model with static and dynamic design will be needed (Figs. 10 and 11).

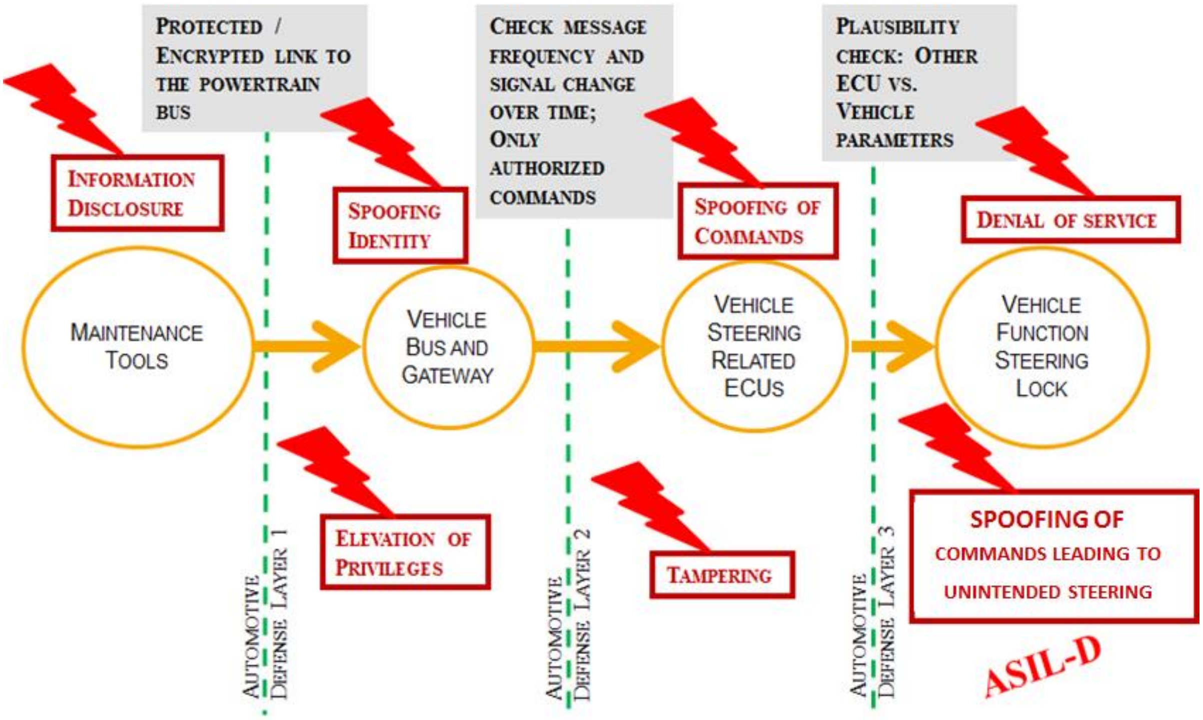

PROTECTED / ENCRYPTED LINK TO THE POWERTRAIN BUS
CHECK MESSAGE FREQUENCY AND SIGNAL CHANGE OVER TIME; ONLY AUTHORIZED COMMANDS
PLAUSIBILITY CHECK: OTHER ECU VS. VEHICLE PARAMETERS
INFORMATION DISCLOSURE
SPOOFING IDENTITY
SPOOFING OF COMMANDS
DENIAL OF SERVICE
MAINTENANCE TOOLS
VEHICLE BUS AND GATEWAY
VEHICLE STEERING RELATED ECUS
VEHICLE FUNCTION STEERING LOCK
ELEVATION OF PRIVILEGES
TAMPERING
SPOOFING OF COMMANDS LEADING TO UNINTENDED STEERING
ASIL-D
AUTOMOTIVE DEFENSE LAYER 1
AUTOMOTIVE DEFENSE LAYER 2
AUTOMOTIVE DEFENSE LAYER 3

Figure 10. Static Auto DLs (Defence Layers) of the Electronic Steering System [14, 16].

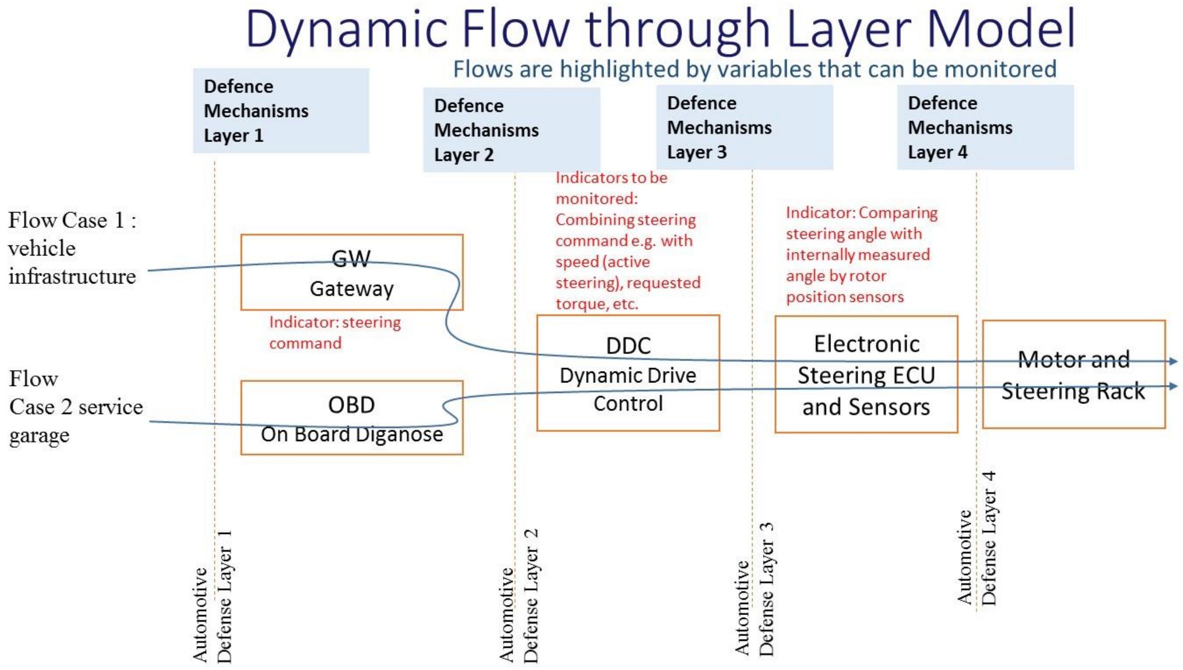

Dynamic Flow through Layer Model
Flows are highlighted by variables that can be monitored
Defence Mechanisms Layer 1
Defence Mechanisms Layer 2
Defence Mechanisms Layer 3
Defence Mechanisms Layer 4
Indicators to be monitored: Combining steering command e.g. with speed (active steering), requested torque, etc.
Indicator: Comparing steering angle with internally measured angle by rotor position sensors
Flow Case 1 : vehicle infrastructure
GW Gateway
Indicator: steering command
DDC Dynamic Drive Control
Electronic Steering ECU and Sensors
Motor and Steering Rack
Flow Case 2 service garage
OBD On Board Diganose
Automotive Defense Layer 1
Automotive Defense Layer 2
Automotive Defense Layer 3
Automotive Defense Layer 4

Figure 11. Dynamic signal flows across layers highlighted by specific variables that can be monitored [14, 16].

In the working party SOQRATES the existing Automotive SPICE 3.0 standard has been integrated with additional questions to cover functional safety (based on ISO 26262:2011) and cybersecurity (based on SAE J3061). An example for BP1 and BP4 (BP ... Base Practice) for SYS.2 System Requirements Analysis is described below [14,16].

Below you find an example integration of Automotive SPICE base practices with ISO 26262 based safety related questions and SAE J3061 cybersecurity related questions for 2 base practices. The SOQRATES working party elaborated this for all engineering (SYS, SWE in ASPICE 3.0) processes.

SYS.2 System Requirements Analysis

ASPICE 3.0 base practice:

SYS.2.BP1: Specify system requirements.

> Use the stakeholder requirements and changes to the stakeholder requirements to identify the required functions and capabilities of the system. Specify functional and non-functional system requirements in a system requirements specification. [OUTCOME 1, 5, 7]
>
> NOTE 1: Application parameter influencing functions and capabilities are part of the system requirements.
>
> NOTE 2: For changes to the stakeholder's requirements SUP.10 applies

Extended Functional Safety Questions:

Related to ISO 26262 clauses ISO 26262-4 6.4.1.1, 6.4.1.3, 6.4.1.4

- Are technical safety requirements in line with the functional safety requirements (Requirements, interfaces, constraints …)?
- Are all technical safety requirements marked as safety requirements and referred to their source (ISO 26262, ECE, FMVSS, …)?
- Are semiformal notations used for ASIL C and D?

Related to ISO 26262 clauses 6.4.2 Safety mechanisms, 6.4.2.1, 6.4.2.2, 6.4.2.3

- Does the technical safety concept specify the necessary safety mechanism and control/monitoring systems to achieve all safety goals on time immediately or by warning/degradation concept, including correct prioritization and conflicting safety strategy?
- Are all relevant measures specified to detect all possible failures/failure combinations including all operation modes and interactions with other systems/items?

Related to ISO 26262 clauses ISO 26262-4, 6.4.4.1, 6.4.4.2, 6.4.4.3

- Only applicable for ASIL C/D requirements. Are the safety mechanisms specified to prevent faults from being latent?
- Only applicable for ASIL C/D requirements. Is the multiple-fault detection interval specified to avoid multiple-point failures and to be consistent with the avoidance of latent faults?

Extended Cybersecurity Questions (SAE J3061:2016):

Related to SAE J3061:2016, clauses 8.4.2 System Level Vulnerability Analysis, 8.3.7 Concept Phase Review, 8.3.6 Initial Cybersecurity Assessment

- Deriving cybersecurity requirements from System Level Vulnerability Analysis
- Definition of Cybersecurity Concept, Functional Cybersecurity Requirements, Cybersecurity Plan, Feature Definition, Threat Analysis and Risk Assessment, Cybersecurity Assessment
- Do regular cybersecurity reviews lead to the identification of new threats and the definition of additional cybersecurity requirements

ASPICE 3.0 base practice:

SYS.2.BP4: Analyse the impact on the operating environment.

Identify the interfaces between the specified system and other elements of the operating environment. Analyse the impact that the system requirements will have on these interfaces and the operating environment. [OUTCOME 3, 7]

Extended Functional Safety Questions:

Related to ISO 26262 clauses ISO 26262-4, 6.4.1 Specification of the technical safety requirements:

- The technical safety requirements shall be specified in accordance with the functional safety concept, the preliminary architectural assumptions of the item and the following system properties:
  a) the external interfaces, such as communication and user interfaces, if applicable;
  b) the constraints, e.g. environmental conditions or functional constraints; and
  c) the system configuration requirements
- Is there an HSI (Hardware Software Interface) specification

Extended Cybersecurity Questions (SAE J3061:2016):

Related to SAE J3061:2016, clauses 8.3.1 Feature Definition

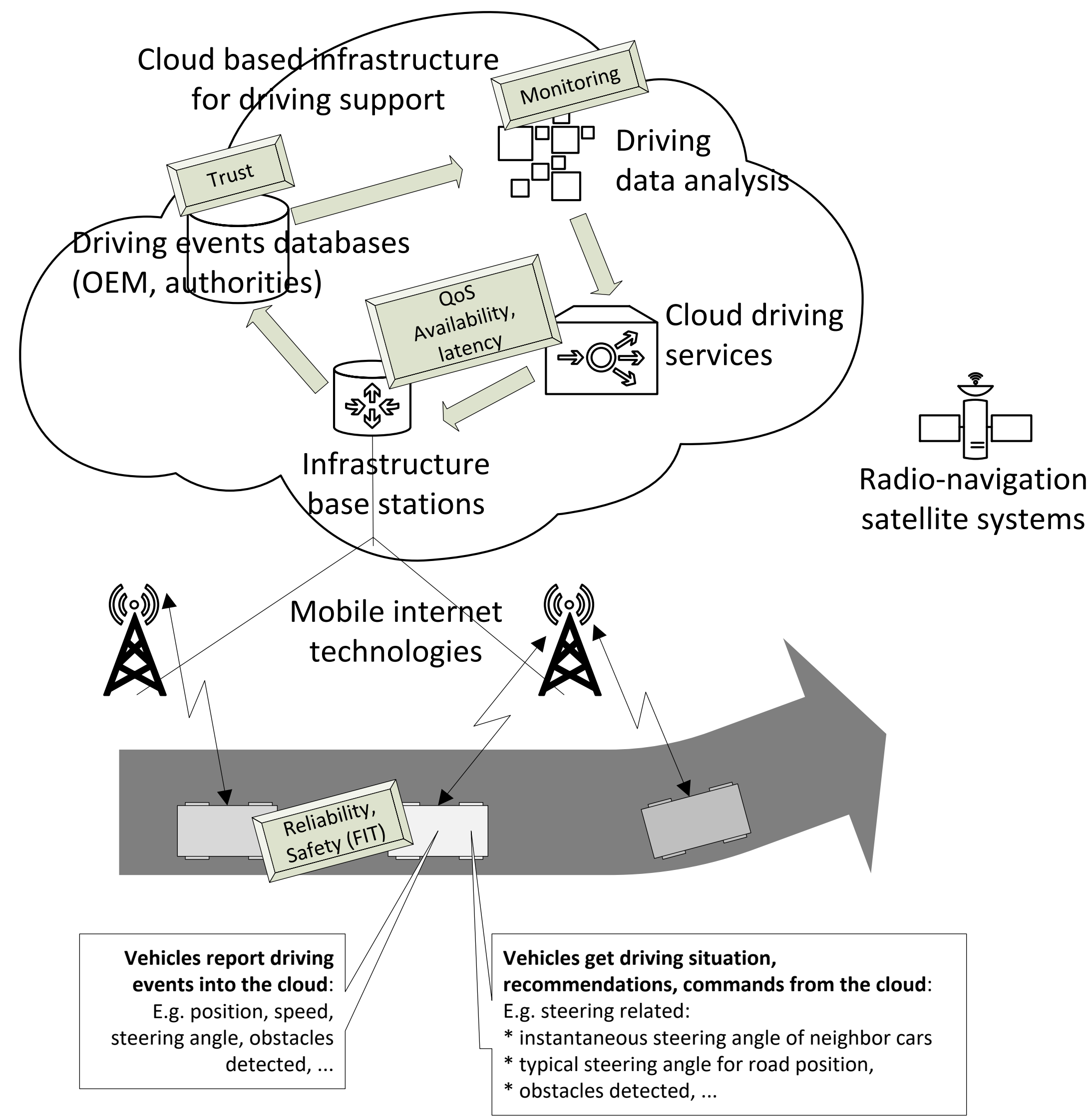
- The feature definition identifies the physical boundaries, Cybersecurity perimeter, and trust boundaries of the feature, including the network perimeter of the feature.
- The feature definition defines the scope and interfaces of the feature.

5 The New Infrastructure Constraints and Processes

In a connected self-driving scenario, cars are connected to global services as part of their infrastructure. Connection technologies heavily base on well-established mobile internet technologies. Connectivity can be considered available for most of the time, but not for 100%. Disconnections can take place at any time, and cannot be controlled. That implies, in-car systems have to be capable of maintaining some mode of safe operation even when suddenly disconnected.

Cars determine their position using a result fusion of more than one positioning system, thereby improving position accuracy. Navigation satellite systems based on GPS, Glonass, Galileo, and more, are well established and globally available. Supplementary technologies include RSS based positioning using mobile internet base stations, and other systems.

When connected, cars can report and receive data to and from cloud services that operate on a fleet level, as well as communicate with – nearby - other cars and infrastructure. As mobile internet technologies are well established and omnipresent in new cars, it can be used for C2X communication in addition to direct communication technologies.



Vehicles report driving events into the cloud: E.g. position, speed, steering angle, obstacles detected, ...

Vehicles get driving situation, recommendations, commands from the cloud:
E.g. steering related:
* instantaneous steering angle of neighbor cars
* typical steering angle for road position,
* obstacles detected, ...

Figure 12. Generic Service Infrastructure Architecture Framework

Cars reporting to a fleet-level infrastructure can supply a broad range of driving, environment, and sensor events together with the car identification and position to the cloud infrastructure. On this level it becomes possible to analyse data on overall fleet level, and – even more interesting for many ADAS applications – this analysis can include the car position. In turn, cars can receive for their current position both fleet-typical car behaviour under certain environmental conditions (matching the current conditions), and any real-time exceptional conditions (e.g. accident warnings, deviations of nearby cars from normal behaviour).

5.1 Infrastructure Based Functions

Let us extend the above steering systems by connecting to the infrastructure services like in **Fehler! Verweisquelle konnte nicht gefunden werden.**2. The interaction between cars and this infrastructure would work like follows.

Cars continuously report a number of steering related sensor and signal data to the infrastructure. These signals include e.g. the current steering angle, speed, car rotation (3D), acceleration (3D), position, etc. A number of car features are involved in collecting this data (steering, ABS, ESP, positioning, Camera/Radar/Lidar etc.).

As part of the infrastructure services, a fleet-typical or even optimal time series of speed, steering angle, etc. can be calculated for each position and an interesting vicinity.

Assuming now an autonomous vehicle cornering manoeuvre, a car receives a recommended time series of steering angles for its current position and the near future on the planned trajectory. Regular refreshes/updates are needed in turn to move forward along the planned path – and faithfully keep the car on track.

Certainly, this mechanism still has to be augmented to correctly react to environmental conditions that impact vehicle dynamics (rain, icy road), and sudden, unplanned, singular events (obstacles ahead, crash, also authority-imposed commands like enforced limiting of speed, etc.). Environmental conditions are sensed locally by in-car systems, by other car's sensors in vicinity, infrastructure sensors, and weather warnings from other sources. Similarly, singular events can be derived from local, nearby, and other behaviour, sensors, commands.

When looking at the critical signal path of steering in the overall scenario, we observe that the path we have to trust

1. Starts from local vehicle sensors (correctness),
2. Continues to signals sent into the service infrastructure (correctly related to position etc.)
3. Where they are stored, and
4. Merge with signal values from cars (danger of data poisoning) in the current vicinity and those ever operated near the current position (depending on the algorithm for driving data analysis, and its correctness).
5. Up-to date steering angles for the current position and road conditions are transferred to all the cars, including the local (availability, low latency, correctness, scalability). See **Fehler! Verweisquelle konnte nicht gefunden werden.** for optimized trajectory vs. potential impact of high latency.
6. Steering angle is applied to the cars' steering as received from the infrastructure (correctness in the current situation).

In the spirit of functional safety we have to ask for QoS (Quality of Service) and monitoring of the infrastructure services to assure correct operation, availability, scalability and low latency. Mind the fact, we want to trust the incoming steering commands and finally apply them to physical steering. Steering related systems are among the most safety critical systems and rated ASIL-D.

In the case of interruption of connectivity, the local car systems suddenly find themselves alone and must be able to ensure continued safe operation. This is especially challenging when e.g. it was part of a platooning cluster of cars just before, and suddenly in disconnected mode yet still located in the middle of the platoon.
Because cars are now all connected together via the described service infrastructure, cybersecurity considerations become complex as we have to protect e.g. from wrong data being injected, services being spoofed, stored data and algorithms tampered with, as well as communication messages being altered along the entire chain of signalling.

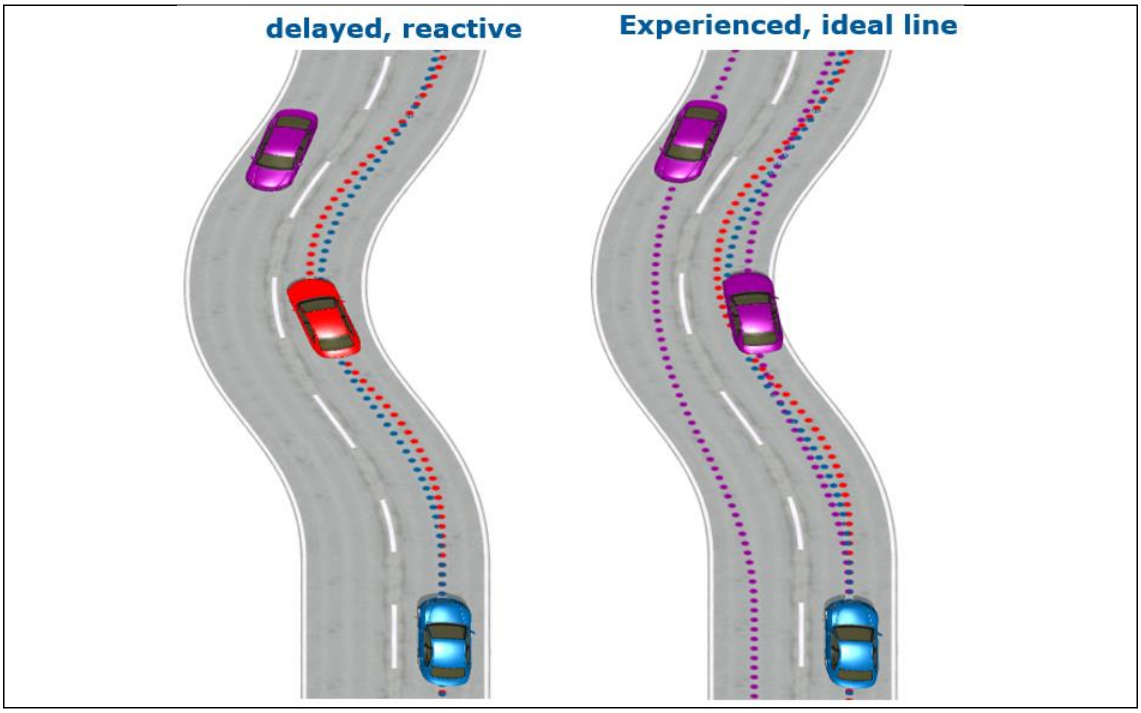


Figure 13. Cornering trajectories compared: reactive/delayed steering (e.g. due to high latency), experienced/optimal

5.2 Extending Assessment Models to Assess Infrastructure

Such an ADAS based infrastructure will require an additional life cycle to considered for the plugin concept of annex D in Automotive SPICE 3.0. The ASI (Automotive Service Infrastructure) processes are connected with the related SYS.1 – SYS.5 cycle in Automotive SPICE, including processes such as ASI.1 Requirements Elicitation, ASI.2 ASI Requirements Analysis, ASI.3 ASI Architectural Design, ASI.4 ASI Integration and Integration Test, and ASI.5 ASI Qualification Test.

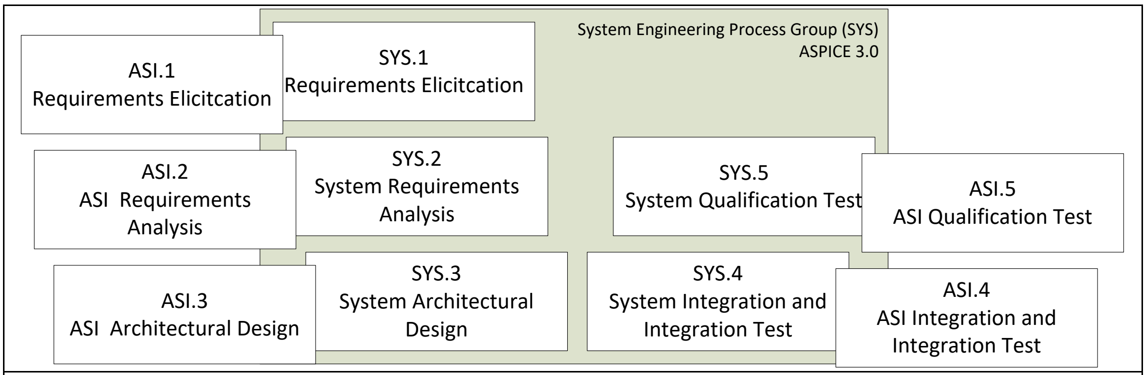

System Engineering Process Group (SYS)
ASPICE 3.0
ASI.1
Requirements Elicitcation
SYS.1
Requirements Elicitcation
ASI.2
ASI Requirements Analysis
SYS.2
System Requirements Analysis
SYS.5
System Qualification Test
ASI.5
ASI Qualification Test
ASI.3
ASI Architectural Design
SYS.3
System Architectural Design
SYS.4
System Integration and Integration Test
ASI.4
ASI Integration and Integration Test

Figure 1 Extension of Automotive SPICE 3.0 with processes ASI.1-ASI.5 for Automotive Service Infrastructure

Figure 14. Extension of Automotive SPICE 3.0 with processes ASI.1-ASI.5 for Automotive Service Infrastructure

In the working party SOQRATES the partners are confronted with new test tracks where self-driving is tested and the vehicle infrastructure supports the ADAS mode. This will lead to a further extension of Automotive SPICE 3.0 so that e.g. the SYS.2 process will have a corresponding ASI.2 process asking related questions about the interfaces to the vehicle infrastructure.

The additional criteria to be asked can be illustrated with the below example of an ASI.BP4 base practice. Compare with the example of “**SYS.2.BP4: Analyse the impact on the operating environment” in section 4 of the paper.**

ASI.2.BP4: Analyse the interfaces between the vehicle and the service infrastructure.

> Identify the interfaces between the vehicle and the service infrastructure. Analyse the impact that the service infrastructure interfaces will have on the vehicle operating environment.
> OUTCOMES: Quality of Service (Availability), Defined reaction in case of no availability, criticality of information, safety classification (if provided as QM or validated among a set of data to be provided with an ASIL), encryption and identification mechanisms to be implemented.

Related ASPICE 3.0 Base Practice:

Related to SYS.2.BP4: Analyse the impact on the operating environment: Identify the interfaces between the specified system and other elements of the operating environment. Analyse the impact that the system requirements will have on these interfaces and the operating environment. [OUTCOME 3, 7]

Extended Cybersecurity Questions (SAE J3061:2016):

Related to SAE J3061:2016, clauses 8.3.1 Feature Definition

- The feature definition identifies the physical boundaries, Cybersecurity perimeter, and trust boundaries of the feature, including the network perimeter of the feature.
- The feature definition defines the scope and interfaces of the feature.

6 Conclusion

The paper illustrates that by using the infrastructure as an input there will be significant changes in the design of the vehicle, the design of the infrastructure, the algorithms used to control a car.

Infrastructure functions will influence vehicle functions which impact the features in ECUs in the car and the new architectures will include views integrating all norms, such as a systems architecture (Automotive SPICE), an infrastructure architecture (proposed extension of Automotive SPICE), a technical safety concept and a technical cybersecurity concept.

Also in future instead of components the infrastructure, vehicle and ECU functions will get an ASIL and a Threat level assigned.

The SOQRATES group will continue this analysis and either ASI processes will be defined or the additional aspect of vehicle infrastructure will be added as a further subset of questions to each base practice.

7 Acknowledgement

The European project AQU (Automotive Quality Universities, 2015-1-CZ01-KA203-013986, 2015- 2017) is co-funded by the European Commission in the Erasmus+ Program. We are grateful for the support.

We are grateful to the experts who have contributed to the SOQRATES working group:

Alexander Much, Elektrobit AG, Andreas Kager, AVL LIST GmbH, Andreas Riel, EMIRAcle c/o Greno-ble Alpes University & ISCN, Armin Rieß, BBraun, Bernhard Sechser, Methodpark AG, Christian Kreiner, TU Graz & ISCN, Damjan Ekert, ISCN GesmbH / LTD, Frank Hällmayer, Software Factory, Frank Kö-nig, ZF Friedrichshafen AG, Georg Macher, AVL LIST GmbH, Gerhard Griessnig, AVL LIST GmbH, Heidi Galle, ZF Friedrichshafen AG, Helmut Zauchner, KTM Motorsport AG, Ivan Sokic, Continental Automotive, Jens Palluch, Methodpark AG, Klaudia Dussa-Zieger, Methodpark AG, Ludger Borgmann, HELLA, Lutz Haunert, Giesecke & Devrient, Martin Böhner, Elektrobit AG, Michael Brasse, HELLA, Peter von Bronk, Best Practice SWQ, Philipp Schmidt-Weber, TDK & EPCOS, Rainer Dreves,Continental Automotive, Rene Obendrauf, AVL LIST GmbH, Richard Messnarz, ISCN GesmbH / LTD, Rudolf Grave, Elektrobit AG, Stephan Habel, Continental Automotive, Werner Aschenberger, KTM Motorsport AG, Christian Santer,AVL, Katharina Lohmann,HELLA, Martin Dallinger, ZF Friedrichshafen AG, Alastair Walker, LORIT LTD, Michael Ochse, BBraun, Ernst Bressau, BBraun, Mate

Bocz, BBraun, Silvana Mergen, EPCOS & TDK, Thomas Wegner, ZF Friedrichshafen AG

8 Literature

[1] 1. Automotive SPICE 3.0, www.automotivespice.com, 2015.

[2] 2. ISO - International Organization for Standardization. “ISO 26262 Road vehicles Functional Safety Part 1-10”, 2011.

[3] 3. ISO - International Organization for Standardization. “IEC 61508 Functional safety of electrical/ electronic / programmable electronic safety-related systems”.

[4] 4. ISO - International Organization for Standardization. “IEC 60812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)”, 2006.

[5] 5. ISO - International Organization for Standardization. “IEC 61025 Fault tree analysis (FTA)”, December 2006.

[6] 6. ISO – International Organization for Standardization. “ISO CD 26262-2017 2nd Edition Road vehicles Functional Safety”, to appear.

[7] 7. G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, “SAHARA: A security-aware hazard and risk analysis method," in Design, Automation Test in Europe Conference Exhibition (DATE), 2015, pp. 621-624, March 2015.

[8] 8. Microsoft Corporation. The STRIDE threat model, 2005.

[9] 9. Macher, G., Armengaud E., Brenner E. & Kreiner, C. “A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context”, Computer Safety, Reliability, and Security - 35th International Conference, SAFECOMP 2016, Proceedings, Springer International Publishing, 2016.

[10] 10. Macher, G.; Hoeller, A.; Sporer, H.; Armengaud, E. & Kreiner, C. Koornneef, F. & van Gulijk, C. (Eds.) “A Comprehensive Safety, Security, and Serviceability Assessment Method”, Computer Safety, Reliability, and Security - 34th International Conference, SAFECOMP 2015, Proceedings, Springer International Publishing, 2015.

[11] 11. SOQRATES, Task Forces Developing Integration of Automotive SPICE, ISO 26262 an d SAE J3061, http://soqrates.eurospi.net/

[12] 12. Macher, G.; Riel, A. & Kreiner, C. “Integrating HARA and TARA - How does this fit with Assumptions of the SAE J3061”, Software Quality Professional, 2016.

[13] 13. Messnarz, R.; Kreiner, C. & Riel, A. “Integrating Automotive SPICE, Functional Safety, and Cybersecurity Concepts: A Cybersecurity Layer Model”, Software Quality Professional, 2016.

[14] 14. Messnarz, R; Kreiner2 ,C.; Riel, A.; et.al, Implementing Functional Safety Standards has an Impact on System and SW Design - Required Knowledge and Competencies (SafEUr), Software Quality Professional, 2015

[15] 15. Macher, G.; Sporer, H.; Brenner, E. & Kreiner, C. “Supporting Cyber-security based on Hardware-Software Interface Definition Systems”, Software and Services Process Improvement - 23nd European Conference, EuroSPI 2016 Proceedings, Springer, 2016.

[16] 16. G. Macher, R. Messnarz, C. Kreiner, et. al, Integrated Safety and Security Development in the Automotive Domain, Working Group 17AE-0252/2017-01-1661, SAE International, June 2017

[17] Felix Redmill, Understanding the Use, Misuse and Abuse of Safety Integrity Levels, Proceedings of the Eighth Safety-critical Systems Symposium, Southampton, UK. Springer, 8-10 February 2000.

[18] Dieter Becker, KPMG International Head for Automotive, Metalsmith or Grid Master: The automotive industry at the crossroads of a highly digitalized age, International Study, kpmg.com/automotive, 2016

[19] Eric Verhulst, Bernhard Sputh, Pieter Van Schaik, Antifragility: systems engineering at its best, Springer International Publishing Switzerland 2015, 17 November 2017

[20] Dario Amodei, Chris Olah, Jacob Steinhardt, Paul Christiano, John Schulman, Dan Mane, Concrete Problems in AI Safety, arXiv Journal, 21 June 2016

[21] Nidhi Hakdra, Susan M. Paddock, Driving to Safety – How Many Miles of Driving Would it Take to Demonstrate Autonomous Vehicle Reliability?, Rand Corportation Research Report, www.rand.org, 2016

[22] Bachmann, V.O., Messner, B., Messnarz, R., 2011. Adapting the FMEA for Safety Critical Design Processes. In: Connor, R.V., Pries-Heje J., Messnarz, R. (eds.): Systems, Software and Services Process Improvement. Proceedings of the 18th European Conference EuroSPI 2011, Roskilde, Denmark, June 2011, Springer CCIS 172, Springer Verlag, pp. 290-297.

[23] Alexander Much, Automotive Security: Challenges, Standards and Solutions, Software Quality Professional, September 2016

[24] Böhner M., Much A.: Extending software architectures from safety to security. Proceedings of the Automotive Safety & Security Conference, 2015. Electronic Proceedings

Lean Layout Kaizen Case Study to Create One-Piece-Flow and Prepare for Pull Implementation in a Company Experimenting Lean Transformation

Marcelo Machado da Silva, Iara Tammela
Departamento de Engenharia
Universidade Federal Fluminense
Rio das Ostras, Brazil
marcelomsilva@gmail.com, iaratammela@gmail.com

Abstract

This paper describes a case study of a Kaizen executed in a value stream layout re-design, with the objective of creating flow and preparing for pull implementation in a company that has few Lean concepts implemented. The new layout will be the first one in the company to follow the Lean concepts, serving as a model for its other plants and processes. The redesign of the layout resulted in 35% less area usage and 20% higher productivity (pieces/man hour) at a lower investment cost, than the initial proposal that the company had in hand to invest. The paper can be used as a reference for other practitioners in the execution of a similar project, especially if the flow organization in the initial situation has isolated operators. The main steps of the Kaizen were to check the initial situation of the layout and manual cycle time, propose a new one-piece-flow organization, balance the operators using the Standard Work Combination Sheet, and create a full size mock-up of the layout for further adjustments. The design of machines, ergonomic analysis and implementation of pull are the next steps to be executed by the team.

Keywords

One-Piece-Flow; Kaizen; Lean; Layout Design; Operator Balancing; Productivity; Standard Work Combination Sheet

1 Introduction

Lean is implemented in many companies with the objective of waste reduction and productivity improvement by constant removal of non-value added activities. Some companies have transformed its processes in the past, especially in the automotive sector. In [1], a chapter of the book is dedicated to describing the Lean implementation in Porsche, and a surprising fact is that it was only in 1994 that “a Porsche Carrera rolled off the line with nothing wrong with it”. In other sectors, however, Lean is still not a reality. Lean is associated with superior performance of companies, leading to competitive advantages and, as stated by [2] “Lean production will be the standard manufacturing mode of the 21st century”. However, in [3] we see that a lot has been learned about the application of Lean tools, with some success, but not many Lean Enterprises have been created. Many companies are still experimenting Lean transformation, but the success factors for Lean implementation are still under discussion in many different articles such as [4], [5], [6], and others.

According to [7], Lean Manufacturing is a waste reduction technique - as suggested by many authors; in practice, however, Lean manufacturing maximizes the value of the product through minimization of waste. [7] also states that the presence of Lean principles defines the value of the product/service as perceived by the customer, and then makes the flow in-line with the customer pull, and makes the company strive for perfection through continuous improvement to eliminate waste by sorting out Value Added activity (VA) and Non-Value Added activity (NVA).

Still according to [7], the sources for the NVA activity wastes are Transportation, Inventory, Motion, Waiting, Overproduction, Over-processing and Defects. The NVA activity waste is a vital hurdle for VA activity. Elimination of these wastes is achieved through the successful implementation of Lean elements[7]. Toyota made respect for people one of the pillars of the Toyota Way (the other one is continuous improvement). “We hire smart people, we give them great latitude in how they do their work because we trust them, and we hold them to objective measures of performance. That’s respect for people” [8].

According to [9] examples of Lean tools are 5S, Value Stream Mapping, SMED (…) Poka-yoke (which is error-proofing), and Autonomation (which means automating and giving machines enough intelligence to recognize when they are working abnormally and flag this for human attention). These tools result in greater productivity, quality, and profits achieved with minimal cost, time, and effort invested. The improvement in a Lean company is done via Kaizen, which means change for better, translated by [10] as continuous improvement, in which teamwork will continuously improve the way the company works. Kaizen can happen in a small daily meeting – if people decide to bring small daily improvements, or in a workshop, where a team will focus on solving one specific problem for a period of time.

In [1], the author describes how the implementation of Lean is related to working in Value Streams, and [11] states that process improvement includes the better use of human effort. This study case shows in practice how the implementation of flow brings better use of human effort, via productivity increase without drastic changes to the technology; and as a future step, the ergonomic analysis will improve the use of human effort in the cell to higher levels. This will be achieved by a case study of a Kaizen executed in a value stream layout redesign, with the objective of creating flow and preparing for pull implementation; the Kaizen took place in a company that has few Lean concepts in place. The new layout will be the first one in the company to follow the Lean concepts, serving as a model for its other plants and processes. Also, the paper aims to provide guidelines for other practitioners looking to execute a Kaizen for layout definition in their companies.

This paper includes a brief description of the company, followed by a discussion of the methodology to be used in a lean layout development workshop by joining the Kaizen methodology with the Lean layout concepts. Finally, the case study is described with the results obtained and future steps proposed.

2 The Company

CANASTRA S.A. is a private company and employs more than 10,000 people in different countries in Europe and Africa. It offers products under different brands, which have been acquired over time, and some of them are more than 200 years old.

In the past 10 years, the company closed many different locations to simplify its production system, and as part of a plan to become more profitable. Last year, a benchmark was made within the sector and CANASTRA S.A. found out that it needs a 30% increase in productivity to be on a par with its competitors. This is similar to the situation Taiichi Ohno encountered in Toyota when he visited the factories in the USA, as described in [12]. Lean Management implementation is, thus, the cornerstone of CANASTRA S.A.'s plan.

The business of CANASTRA S.A. is not within the automotive sector, which means that Lean Management is still not a reality in most of the supply chain and equipment providers. The company, thus, has requested that the industry be kept anonymous, so that the competitive advantage is kept for longer. In CANASTRA S.A., Lean implementation began in 2009; the process lost some of its momentum for some time, and the company focused on just one plant. In 2015, the results obtained in this plant (especially in terms of quality) were enough to gain management approval to boost the implementation for deployment in all other plants. The creation of a corporate Lean department – initially with three employees, who are responsible for the implementation in the different sites – is the biggest indicator that the top management level supports the implementation of Lean within CANASTRA S.A.

CANASTRA S.A. has a clear objective: to become a profitable company within 3 years; the company also needs to grow after years of declining sales and increasing debt. The company has, in the past years, executed a strategy to lower costs, which meant losing control of different aspects of the business: the catalogue has many different products with similar designs (some of which compete with each other) in different price segments; and factories in different countries have run most activities in product development, sales, marketing, and portfolio separately, so there is no global approach to their business strategy.

Inside the factories, all layouts are functional, with one operator per workstation. There is a lot of WIP between each process and, also, final products in the supply chain (usually the ones that the client did not request). Complex solutions for automation are in place, which shows the paradigm of developing robots to replace humans, rather than organizing the work according to the Lean concepts and improving productivity with simple automation; this is one of the differences between conventional management and Lean management, as described in [13]. 5S, SMED, TPM and standardization are weak, and, when implemented, are only in small areas. Muda is seen at its most simple ways, such as when operators wait for parts, and overproduction is seen everywhere. In general, machines are maintained only when they break down.

Quality is also a big issue in CANASTRA S.A, and only 30% of the products are produced with no rework. This turns traditional production planning even more confusing. Customer delivery is not ideal, regardless of the high stock of finished products, due to the different problems mentioned above – management levels see this as one of the most important points to be improved. In terms of ergonomics, there are unacceptable situations, such as the manual handling of products that weigh above 20kg, also forcing postures and gestures that may cause work related musculoskeletal disorders.

This situation must be seen as positive: it means there are many points to be improved, and that the plan to become more profitable is possible. Lean implementation can bring big productivity improvements in this context, as well as WIP reduction (improving cash flow and lead-time). [14] links Lean to improvements in the four operational dimensions - Quality, Delivery, Flexibility, and Cost; in [15], we see how the implementation of Lean in the suppliers of Honda brought productivity gains of approximately 50%.

Due to the need to replace one important heat treatment oven, the company had the opportunity to completely re-layout one of the 4 product flows of one of the plants, according to the Lean principles, to use it as a pilot for the future projects. This flow produces items that weigh between 15 and 25 kilograms and have sizes up to 90x30x30 cm. This opportunity is the one which will be described by this case study.

3 Methodology

In [1] the author defines that the main steps to implement Lean in a factory are to define value streams, to create flow and to create pull. In this paper, the focus is in creating flow, since the value streams are already defined in the company, and the machines needed to produce the items are known.

According to [1], to create flow one needs to implement the following steps:

- Continuous Flow: Arrange Production steps in sequence;
- One-piece-flow: the product moves from one step to the next, one at a time, with no buffer of work-in-process in between.

Further in [1], the authors discuss the fact that a one-piece-flow means that if one machine stops, the whole flow will stop; it is vital, then, to:

- implement SMED to allow flexible production;
- cross train operators in all tasks of the cell, which enables to separate man and machine;
- define the right size of the machine that is needed, meaning slower and less automated machines;
- implement Pokayoke solutions;
- implement 5S and visual management.

This basically ties all the Lean tools together, and shows that to reach the main goal of creating flow, it will be necessary to implement most other Lean tools. It is important to note that, as described by [16] once a company defines a vision to implement flow in its factories, a policy deployment process shall pull the implementation of each of the necessary tools, which will give different results, rather than pushing the implementation of separate tools in the company (such as a global 5S in the whole plant, but without a vision in mind).

A. Kaizen Workshop Methodology

The Kaizen Workshop Methodology, which follows the PDCA cycle is defined by [10], in which the author separates the Kaizen in three steps: Preparation, Workshop and Sustaining.

In the Preparation Phase, the objective is to define the scope and objectives, understand the current state, collect necessary data, and position all this data inside the team room in a visual design that allows all data to be seen by all participants. The use of computers to arrange this data is not recommended, since it complicates access to the information.

During the Workshop phase the steps are to analyse the current state, develop a future state vision with an action plan to reach this vision, and start implementation. It’s usual for the implementation to happen during the workshop phase.

Finally, the sustaining phase is to check and act, the team needs to verify if the actions that were implemented were effective, and take countermeasures where necessary, to reach the vision.

B. Lean Layout Development

The development of a lean layout is described by [16] in great detail. Initially, the author affirms that there is big resistance to implement a one-piece-flow, since the feeling is that there is too much variability in the factory for it to function in this way. In order to refute this, a Product Quantity analysis is made, showing how many part numbers represent which percentage of the production volumes; usually it shows that few part numbers represent 80% of the volumes. Another important point described by [16] is the design of a layout without considering the operators; if this design considers only the space and the machines available, some consequences will be larger WIP, low visibility of the process, separation between operators (which prevents communication), and an increase in the space needed from 30 to 40%.

The author then suggests the calculation of the number of operators needed to complete the activities by using the formula below:

Minimum number of operators=

$$\frac{\text{Total Manual Cycle Time}}{\text{Design Takt Time}}$$

The author describes the Design Takt Time as the lowest Takt Time expected, or the maximum capacity of the line. The line must, however, allow the production at higher Takt Times, which means smaller capacities, keeping the productivity at each level of production. Once this is defined, the next step is to decide on the number of lines desired to make the product. This will define the size of the cycle of each operator. As an example, adapted from [16] if the Total Manual Cycle Time is 100 seconds and the Design Takt Time is 10, we would need 10 operators to deliver products at the Takt Time. However, the process can be made in one line of 10 operations of 10 seconds, or in two lines of 5 operations of 20 seconds, and so on, as shown in Fig.1. This decision will consider the need for training, which increases as the operations become bigger, and the repetitiveness of the operator’s activity which, according to [16], will bring stress and, usually, high turnover to the company. Further, [16] suggests 30 seconds of cycle time as a low limit to consider the task repetitive, bringing high turnover.

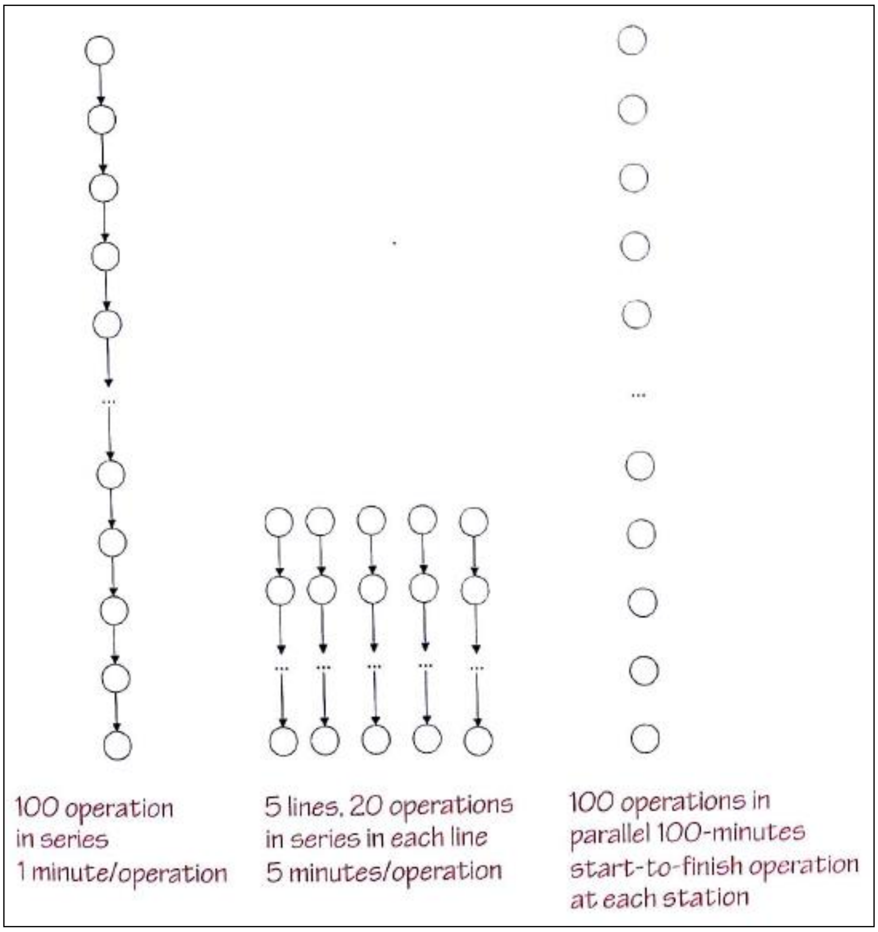


Fig. 1. Possible breakdowns for a 100-minute assembly process [16], pg.51

Once the number of lines or cells has been defined, the next step is to list all the necessary activities, in the order of the process. This order is the one in which each workstation/machine shall be installed in the line, one next to the other. The product moves one piece at a time to the next process, and shall not return to any station after it has passed it (guaranteeing a continuous flow as well as a one-piece-flow).

Next, a line balancing shall be made, to define which steps each operator shall execute. In our example, we had split the production in two lines of 5 operations of 20 seconds each. The quantity of work of each operator must match the Takt Time, and must be the same between all. At this point, each activity shall be analysed for quick wins to remove manual cycle time. The removal of 20 seconds of activity means that one operator can be removed from the line, bringing productivity gains. In this context, the 20 seconds can come from the group of operations; in a production that works in batches and isolated operators, the removal of some seconds from one workstation will bring mostly overproduction or Muda, without increasing productivity. In a second moment, small investments can be made to further reduce the manual operations, with simple automation in all processes, rather than the complete automation of one process, which will usually mean a higher investment and, many times, inflexible equipment, with high changeover times.

The balancing and the layout are linked, since the total work of the operator will depend on the distances between the equipment. It is necessary to reduce the distances as much as possible, usually respecting a minimum distance of one step between each workstation. This forces the operator to take one step, rather than reaching for a tool and causing a bad posture. With the same concern, it can be necessary to redesign current off-the-shelf equipment from the supplier. In [16], the author shows a curing station, which needs a longer distance for its process (Fig. 2). The normal layout is to have the entrance and the exit at opposite sides of the equipment. It is necessary to rethink all equipment so that the product entry and exit are as close as possible to each other, in order to reduce movement by the operator.

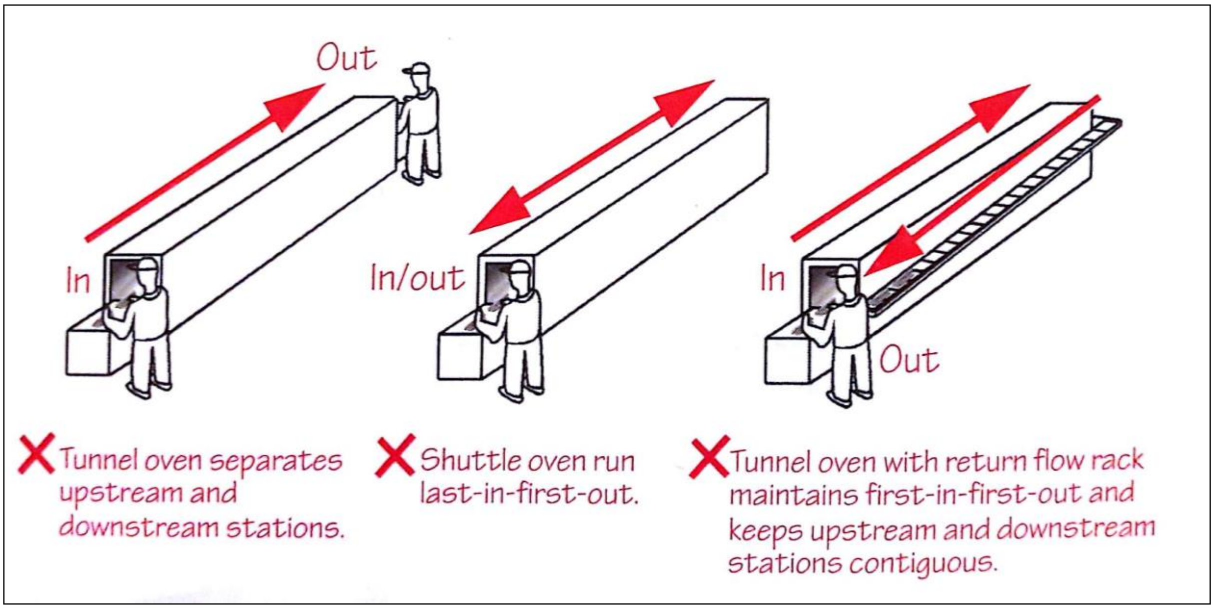

Out
In
In/out
In
Out
✕ Tunnel oven separates upstream and downstream stations.
✕ Shuttle oven run last-in-first-out.
✕ Tunnel oven with return flow rack maintains first-in-first-out and keeps upstream and downstream stations contiguous.

Fig. 2. Curing Station [16], pg.141

At Canastra, this is called the “Daisy Flower Concept”: as Fig. 3 shows, the operators are inside the disk of the flower, while equipment and supplies are the petals. This means that the equipment in the cell can be as big as needed, provided that the in and out locations are next to each other, and in the sequence of the process as shown above. The objective of this is to reduce walking, and allow operators to help each other, communicate, and see quality issues or other problems just as they occur. This concept supports the team when discussing the layout, since the focus is to keep the operations close, while the machines must adapt to this necessity, and not the opposite, as is most common.

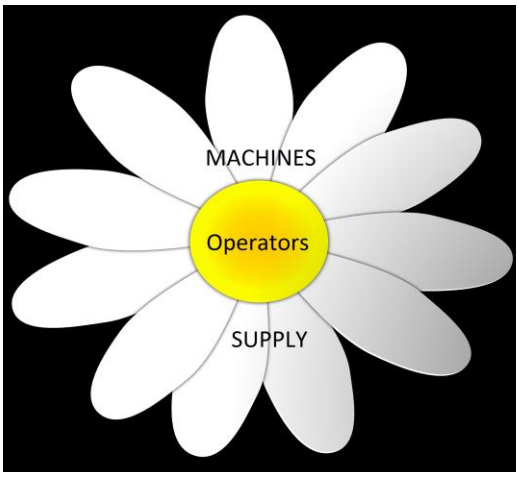


Fig. 3. The Daisy Flower concept for Lean Cells. Created by the authors.

C. Kaizen for Lean Layout Development

The analysis of the Kaizen methodology and the items proposed by [1] together with two more sources, [17] and [18], made possible the proposal of a process to design a new lean layout:

Preparation:

1. Scope and Team definition;
2. Training for Team (Kaizen execution and Flow implementation objectives and method);
3. Current Status design and measures of indicators;
4. Goal Calculation;

Workshop:

5. Future state Layout + operator balancing with iteration process to improve (including quick wins and list of possible investments to reduce total manual cycle time);
6. Full-Scale Mock-up with iteration process and balancing;
7. Presentation and approval;

Implementation / stabilization:

8. Equipment design;
9. Ergonomics analysis;
10. Pull Flow design;
11. Implementation, training and stabilization.

While some authors (such as [17]) use computer simulations to define flows, or to test the designs, the use of a real mock-up simulation is proposed here, since the first Kaizen changes the reality of the Genba completely. Having a real-sized mock-up of the proposed layout will help people to envision the new process, allowing everyone to see and build on the idea; this is supported by [16], who affirms that the operators appreciate this technique.

After implementing the new layout, and once the situation is stable, a new Kaizen can be executed to further reduce Muda, this time with real experience of one-piece flow. The use of simulation and optimization process in a Lean implementation can cause the process to only be understood by those who have the knowledge of the systems; thus, it is preferable to use simple, visual tools; implementation, adjustment, and improvement should be done with experience, and with participation from all levels of the company.

The first expected gains from flow implementation are a higher productivity and a smaller area needed to produce the same volume of products (mainly due to the strong reduction of Muda and WIP). Furthermore, the implementation of flow will allow the company to obtain other gains: a simplified management of the Genba; easier visualization, by those in the company, of non-value added activities; and continuous improvement carried out by all levels of the company.

4 Lean Layout Kaizen Case Study

With constant pressure to improve productivity, CANASTRA S.A has planned investments for the coming years. The focus of these investments are the factories with the highest labour cost. This Kaizen was executed in order to evaluate the existing proposal of a new layout, which includes the following workstations: (in the order of the process) inspection, painting machine, painting robot, and finishing. At the end of the process, the part is loaded onto a large shuttle car that takes the product to a heat treatment oven. The line has to be able to reach a design Takt Time of 60 seconds/piece, but it must also be able to work at slower paces, according to customer demand. The families of products have already been defined in this line.

A. *Preparation*

Fig. 4 shows the initial balancing of the operators. The original layout, shown in Fig. 5, contains a total of four robot arms that are used to move parts between different conveyors, without adding any value; the locations of the operators were not in the initial layout (they were added later, since it is common to focus only on the position of equipment). The operators are isolated in the layout, which does not allow them to help each other, or to share activities, this will make impossible the work at lower productivity levels.

In the preparation phase, the team measured all the manual cycle times of the current operations, and made videos to facilitate analysis during the Kaizen. Indicators were measured and calculated for the initial situation shown in Table I. One difficulty at this point is that there is no laminar flow implemented, which means that the calculation of the takt time is more complex. Although the layout shown has a design takt time of 60 seconds/piece, the pieces are treated in two parallel flows; these are joined for the last operator, who handles pieces from both flows. In the balance chart we have shown that the first two operators work with the process (A), the 3rd and 4th work on the next process (B), while the 5th operator works on the last process (C) for all pieces. This is why the 5th operator has a takt time of 60 s/piece, while the others work at 120s/piece. The manual cycle time shown in Table I is the total manual cycle time needed to produce one item, which means the sum of cycle times from operators 1+3+5, or 2+4+5. So, the information in Table I is separated by flows, and, thus, the takt time shown is 120s/piece, and two flows are required to meet the design takt time of 60s/piece.

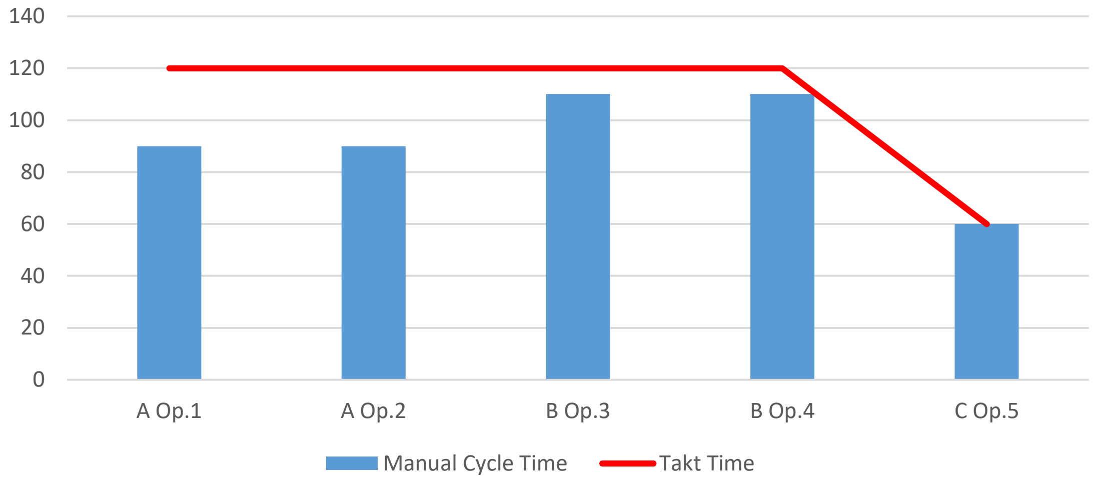


Fig. 4. Initial Balance Chart of the operators, showing disbalance and available time. Created by the authors.

INITIAL STATUS

Indicator	***Before***
# of Operators	5 (Isolated)
# of handling robots	4
Length of conveyors	70m
Area	666m²
WIP	25 pieces
Lead Time	25 minutes
Manual Cycle Time	260s
Design Takt Time	120s/piece

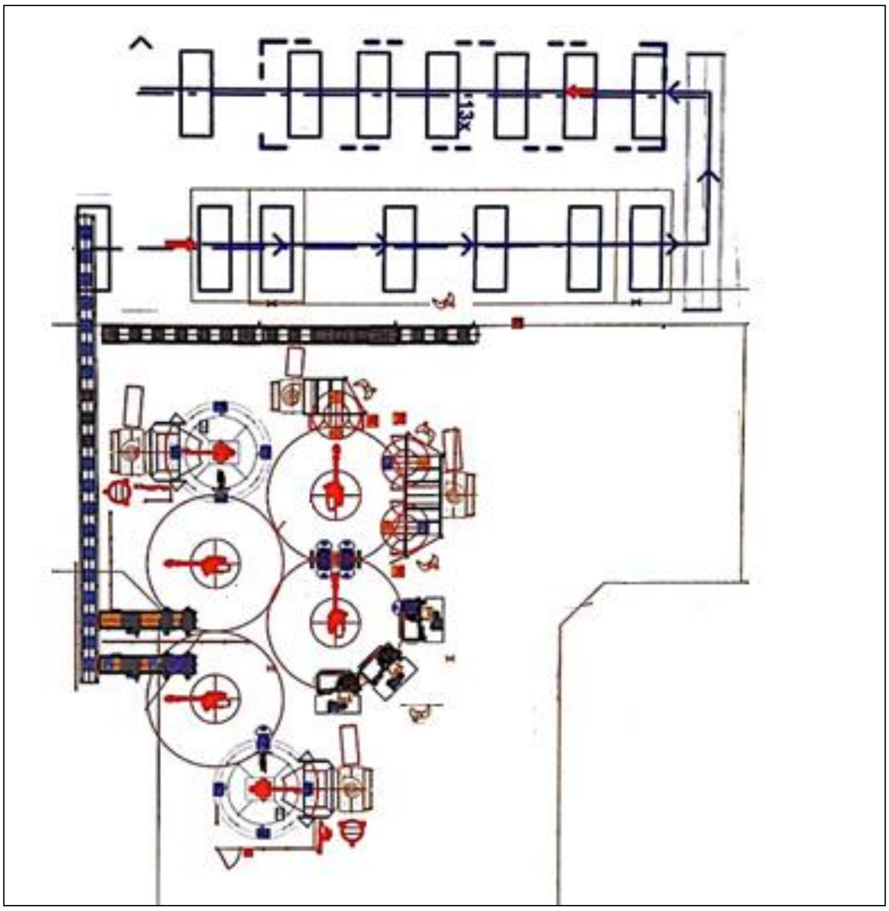


Fig. 5. Initial Layout, with five isolated operators. Created by the authors.

B. *Workshop*

After a short training session, the team defined their goal, is found by dividing the Total Manual Cycle Time by the Takt Time as shown in [16], which is 260/120=2.16 operators. Thus, with the current technology, the team has a goal of reaching a layout with 2 operators for each flow, totalling 4 instead of 5, which is a 20% improvement. To reach this, the total manual cycle time has to be reduced from 260 to 240 seconds.

After implementation, continuous improvement should allow the site to reach an organization of 3 or 2 operators, which would mean a total of 40% or 60% productivity increase, respectively. This is done by constant analysis, with strong participation of the operators, reducing movement, and implementing better tools as well as simple automation to constantly remove manual cycle time from the process.

The team designed a one-piece flow layout, separating the volume required in two distinct flows (due to the size and speed of the painting robot, which has a cycle time of 120s, and positioning the value-added points side by side, using the daisy flower concept. This decision also means that the repetitiveness of the activity for the last operator will be lower, since each cycle for all operators will be of 120s, rather than 60s in the case of the 5th operator in the initial situation. This layout was adjusted in an iteration process with the SWCS sheet, in order to understand how the operators would work together, and with the machines. The simple organization of the layout in a one-piece-flow removed a lot of handling of pieces and walking, and the total manual cycle time was reduced to 202 seconds per flow.

The final proposal of the workshop can be seen in Fig. 6, as a first draft of the technical drawing. It is clear that the final proposal is using much less space, robots and conveyors. To reach this layout, many discussions were made, so everyone would understand the new process. When difficulties appeared, they were written on a list and kept for later discussion, but not to block the development of the solution.

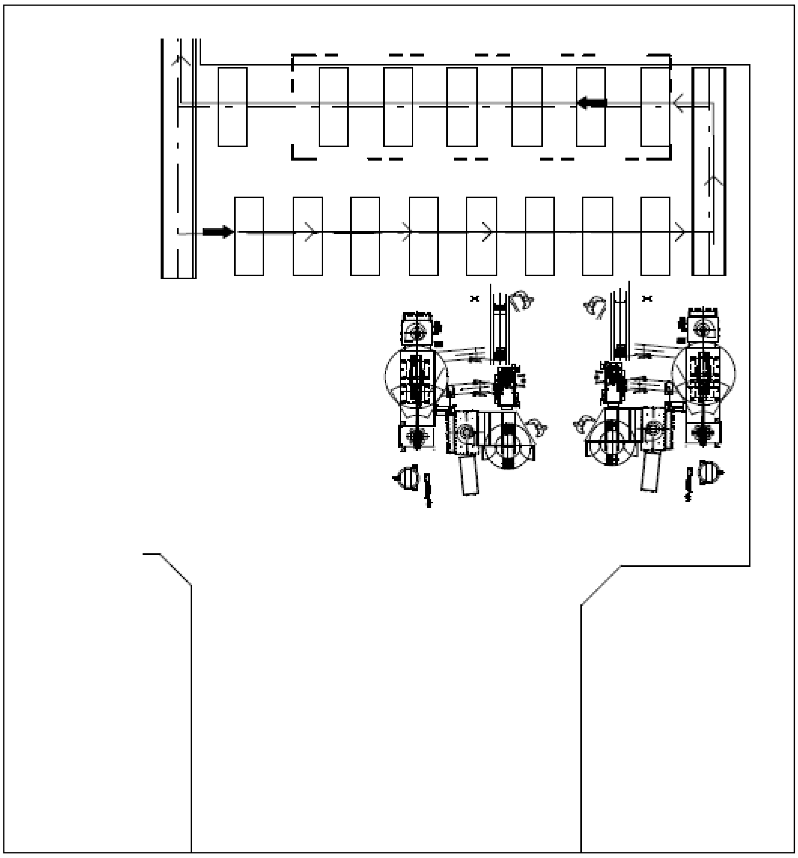


Fig. 6. Proposed layout, showing the large empty area as compared to the initial proposal. Created by the authors.

Fig. 7 shows the balancing in the proposed layout, which respects the daisy flower concept, with all the operators close to each other, and the machines outside of this area. Note that there is still unbalance in the manual cycle time, and the team defined a number of small investments for future analysis; that could be made to reduce the total manual cycle time from 202 seconds to 180 seconds per flow, enabling the execution of all tasks by 3 operators rather than 4. This means that the removal of 22 seconds of manual activities from each flow will bring a productivity increase of a further 25%; it is what allows continuous productivity increases in a lean layout.

However, as described in the next steps of this paper, it will be better if the team is able to join one flow, such as this one, with the final inspection and packaging processes of the same flow, which will allow the team to manage the quality of their products, rather than share the work between different flows of products. Today, these processes are more than 300m apart, which means that communication on quality issues in the final inspection depends on the supervisor.

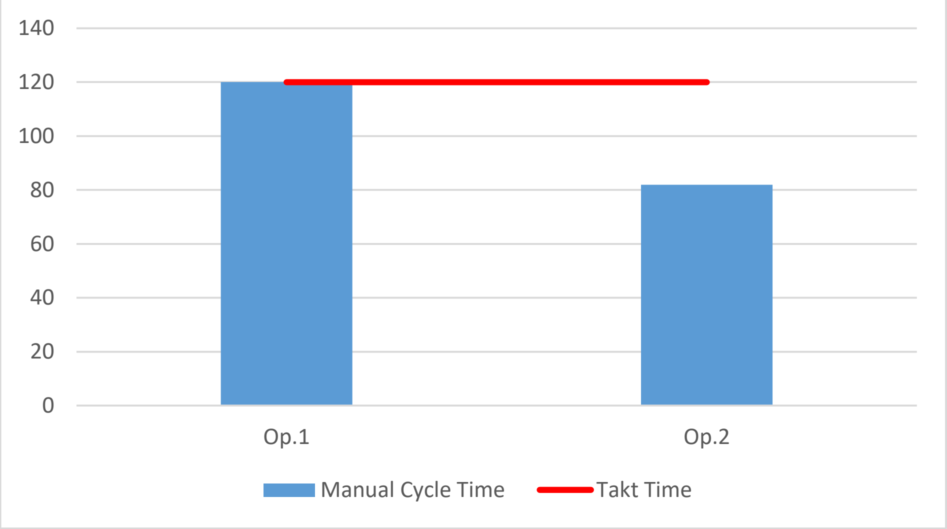
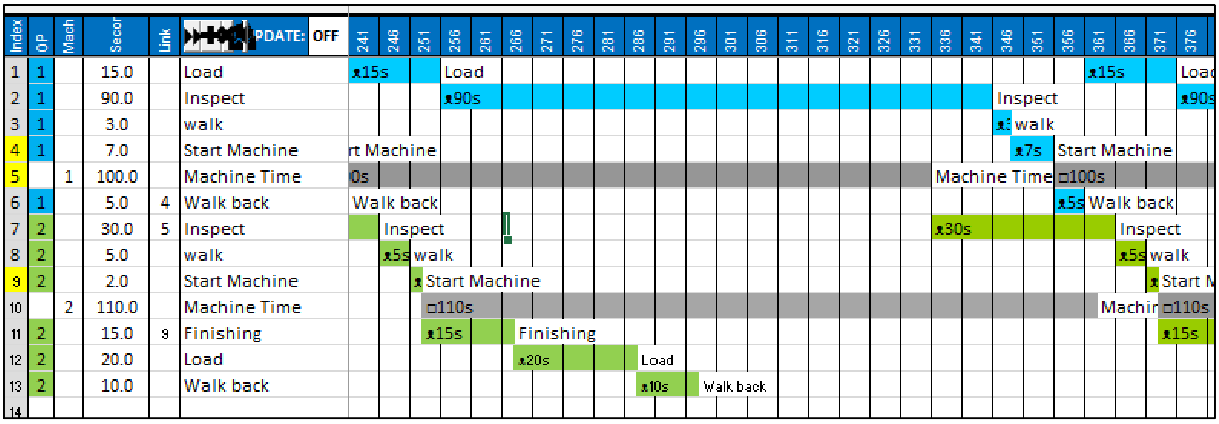


Fig. 7. Balance Chart of operators on proposed layout, still showing opportunities for improvement. Created by the authors.

Fig. 8 shows the SWCS sheet, which is a better tool than the Balance Chart to see the activities of the cell, since it includes the machine times and separates each activity of each operator. This file was discussed many times, relating the proposed layout to the walking distances and the activities. Note that the second operator is kept with a much lower load. The objective is to make it clear that he has to wait, and to avoid overproduction.



Index	OP	Mach	Secor	Link	PDATE: OFF
1	1		15.0		Load
2	1		90.0		Inspect
3	1		3.0		walk
4	1		7.0		Start Machine
5		1	100.0		Machine Time
6	1		5.0	4	Walk back
7	2		30.0	5	Inspect
8	2		5.0		walk
9	2		2.0		Start Machine
10		2	110.0		Machine Time
11	2		15.0	9	Finishing
12	2		20.0		Load
13	2		10.0		Walk back
14					

Fig. 8. SWCS of operators and machines on proposed layout. Created by the authors.

After the definition of the layout, a full-sized mock-up was created, using cardboard and tables. This enabled operators, supervisors and many others to see the proposal and suggest improvements. The team preferred this to a complex simulation model using a software such as Arena, since this way allows everyone to participate in the creation of the model. Furthermore, a simulation is more useful when the variabilities of the process are known, so that shortages can be checked, and, in this case, the company will work to eliminate these variabilities, gaining more productivity with time, rather than planning to absorb them. The proposed layout will make many problems visible; today, they are hidden by inventory and excess capacity. These problems shall be solved one by one, and this brings the company to a new paradigm of workplace organization.

The main deliverables of the workshop were: Layout Proposal, Full size Mock-up, Balance Chart, SWCS sheet, calculated indicators, list of problems to be discussed, list of small investments to reduce manual cycle time, and an action plan for the next steps. These were presented to the plant management at the end of the workshop, in order to give a clear vision of the benefits and the difficulties that the team will face to implement the new layout.

RESULTS AND CONCLUSIONS

A. *Main Results*

MAIN INDICATORS (BEFORE AND AFTER)

Indicator	***Before***	***After***	***Improvement %***
# of Operators	5 (Isolated)	4 (grouped)	20%
# of handling robots	4	2	50%
Length of conveyors	70m	10m	85%
Area	666m²	418 m²	35%
WIP	25 pieces	5 pieces	80%
Lead Time	25 minutes	5 minutes	80%

As shown in Table II, the productivity was improved by 20%; the area was reduced by 35% (exactly as defined in [16]) and the lead time was cut down by 80%. The additional cost of developing the necessary equipment to the specification, rather than off the shelf, is compensated by the removal of 4 handling robots. Most importantly, the investment is calculated to last more than 10 years, so these improvements will enable the company to be more productive and reach its goal of becoming more profitable.

The biggest gain of this workshop is that the new layout enables each flow to work at different levels of productivity, following a rhythm closer to the Takt Time, while maintaining the productivity (pieces/man.h). The operators are also able to work as a team and help each other during the solution of problems within the cell. Also, with continuous improvement in each of the workstations, productivity can be constantly improved.

B. *Main Dificulties*

The training was not long enough, so participants depended too much on the Lean team to show the way. It would have been better to have a longer training to give the team more autonomy on the decisions.

Quality problems mean that at each scrapped part the line stops. The product is very far from a good quality output. The new organization will also help to improve the quality, but it is known that this shall be an issue in the beginning.

Suppliers are not prepared to design equipment that follows the lean concepts. For the equipment development step, a lot will have to be discussed with the suppliers so they manage to create equipment that works well in the designed cell.

People are not used to laminar flow and one piece flow; in the company, they do not think it is possible to work this way. This was the biggest paradigm to break. At the end of the workshop, the participants were convinced that it was possible to work in this new way. They also came to believe that it is possible to solve new problems and reach even better results.

C. Main enablers

Partial top down support: there was strong support from some of the management team, which guaranteed the continuation of the project. However, not all managers and directors agree with the proposed solution, so there are still more people to be convinced before the company invests in the new layout.

People open to new concepts after the creation of trust: this means that after an initial discomfort, the team felt that they could trust each other, and communication became open, clear and sincere.

Investment is already a reality: this workshop was executed because people knew that there was capital to invest in a new layout to bring productivity gains, which is not so common in companies where we must accept the current layout to avoid investments.

5 Next Steps

A. Connection to finishing processes

After the heat treatment, the product goes through inspection and to the final packaging process; these also need to be analysed with a similar methodology. That will allow the two cells to be arranged next to each other, and enable a complete view of the process in a small space. This is especially important for feedback on quality of the products the operators have produced.

B. Equipment Development

The current equipment will not allow the company to implement the Lean concepts; as described in[1], the current available machinery for painting is much larger than needed (and was designed to have 10 products in WIP). In order to enable the implementation of the proposed layout, it will be necessary to execute two equipment design workshops, one for the painting machine and one for the robot. These workshops will bring together equipment suppliers, operators, and maintenance personnel to define the best solution that will fit the needs of CANASTRA S.A.; the solution shall include TPM needs.

C. Ergonomics

There is a need to further improve the ergonomics of the processes. The proposed layout has already reduced much manual handling, but the size and weight of the product make it difficult to handle and inspect without postures and gestures that are not ergonomic. Thus, the use of a tool such as RULA Analysis, as described in [19] and [20], can immediately reduce the strain on the operators, and shall be executed in parallel with the design of the two equipment mentioned above.

D. Pull Flow Implementation

Once the layout is implemented and the flow is created, it will be time to define the system which will pull the production. Because of that, a workshop to design the scheme of flow of the production, with the elements of a Kanban system correctly identified, is also required. To work as closely as possible to the TAKT time, different standards must be made for the cell. They must figure out how to work with 1, 2, 3 or 4 operators, since 4 operators is the maximum capacity of this cell; that will produce the maximum output of 1 part every 2 minutes.

E. Cell Management and Continuous Improvement

Finally, once the cell is implemented, the training of operators has to be executed, as well as the implementation of a daily management routine. The operators need to visualise the results of their work, and work as a team to find and implement improvements; this is one of the big changes in Lean production described by [1]. The group of operators in one cell, or flow, are responsible for their work, and can see the production process from start to finish, in a continuous effort to improve the quality and reduce the muda.

A learning curve will be needed, since a new way to work is going to be implemented; this is expected in the implementation of any new process. The changes of working in one piece flow will make new problems visible to the company; that enables people to find solutions, and, ultimately, brings profits.

6 References

[1] J. P. Womack and D. T. Jones, LEAN THINKING: Banish Waste and Create Wealth in Your Corporation. Free Press, 1996.

[2] R. Shah and P. T. Ward, “Defining and developing measures of lean production,” J. Oper. Manag., vol. 25, no. 4, pp. 785–805, 2007.

[3] J. Womack, Gemba Walks, 1.0. Cambridge, MA: Lean Enterprise Institute, 2013.

[4] B. Noori, “The critical success factors for successful lean implementation in hospitals,” Int. J. Product. Qual. Manag., vol. 15, no. 1, p. 108, 2015.

[5] S. Zargun and A. Al-Ashaab, “Critical Success Factors for Lean Manufacturing: A Systematic Literature Review an International Comparison between Developing and Developed Countries,” Adv. Mater. Res., vol. 845, pp. 668–681, 2013.

[6] T. H. Netland, “Critical success factors for implementing lean production: the effect of contingencies,” Int. J. Prod. Res., vol. 7543, no. October, pp. 1–16, 2015.

[7] R. Sundar, A. N. Balaji, and R. M. Satheesh Kumar, “A review on lean manufacturing implementation techniques,” Procedia Eng., vol. 97, pp. 1875–1885, 2014.

[8] T. H. Netland, J. D. Schloetzer, and K. Ferdows, “Implementing corporate lean programs: The effect of management control practices,” J. Oper. Manag., vol. 36, pp. 90–102, May 2015.

[9] S. A. M. Elmoselhy, “Hybrid lean-agile manufacturing system technical facet, in automotive sector,” J. Manuf. Syst., vol. 32, no. 4, pp. 598–619, 2013.

[10] J. K. Liker and D. Meier, “The Toyota Way,” Action Learn. Res. Pract., vol. 1, no. 22, p. 288, 2015.

[11] W. E. Deming, Out of the Crisis. The MIT Press, 1986.

[12] T. Ohno, Toyota Production System: Beyond Large-Scale Production, vol. 15, no. 2. Productivity Press, 1988.

[13] K. Perbandingan, S. Pembuatan, and B. Satu, “Comparative Study of Manufacturing Strategy between Japanese and Western Approaches : An Overview,” J. Kejuruter., vol. 24, pp. 35–43, 2012.

[14] R. Z. Rasi, U. S. Rakiman, and M. F. Ahmad, “Relationship Between Lean Production Performance in the Manufacturing Industry and,” in IOP Conference Series: Materials Science and Engineering2, 2015, vol. 83, no. 1, pp. 1–10.

[15] J. P. MacDuffie and S. Helper, “Creating Lean Suppliers: DIFFUSING LEAN PRODUCTION THROUGH THE SUPPLY CHAIN.,” Calif. Manage. Rev., vol. 39, no. 4, pp. 118–151, 1997.

[16] M. Baudin, Lean assembly : the nuts and bolts of making assembly operations flow. New York: Productivity Press, 2002.

[17] N. T. Lam, L. M. Toi, V. T. T. Tuyen, and D. N. Hien, “Lean Line Balancing for an Electronics Assembly Line,” in Procedia CIRP, 2016, vol. 40, pp. 437–442.

[18] M. Rother and R. Harris, Creating Continous Flow. An action Guide for Managers, Engineers and Production Associates. Lean Enterprise Institute, 2001.

[19] L. McAtamney and E. Nigel Corlett, “RULA: a survey method for the investigation of work-related upper limb disorders,” Appl. Ergon., vol. 24, no. 2, pp. 91–99, Apr. 1993.

[20] S. S. Gnanavel, V. Balasubramanian, and T. T. Narendran, “Suzhal – An Alternative Layout to Improve Productivity and Worker Well-being in Labor Demanded Lean Environment,” Procedia Manuf., vol. 3, pp. 574–580, 2015.

Benefits of Defect Taxonomies and Validation of a new Defect Classification for Health Software

H. Ketheswarasarma Rajaram[1] , J. Loane[2], S. T. MacMahon[3], F. Mc Caffery[4]
Hamsini.Ketheswarasarma@dkit.ie[1], john.loane@dkit.ie[2], silvana.macmahon@dkit.ie[3], fergal.mccaffery@dkit.ie[4]
Dundalk Institute of Technology, Ireland

Abstract

Defect-based testing is a powerful tool for finding errors in software, including medical device software. Many software manufacturers avoid this method because it requires a detailed defect taxonomy that is expensive to construct and difficult to validate. SW91[1] is new defect taxonomy for health software being developed by the Association for the Advancement of Medical Instrumentation. This paper explains how defect taxonomies have been used and the benefits to industry. The initial steps of the validation of SW91 include mapping vulnerabilities from the Common Weakness Enumeration and a dataset from a medical device software development company in Ireland. Finally, the paper details future plans for validation, including taxonomy based testing which will be used to validate the efficiency, reliability, ability to perform useful analyses and defect coverage of SW91.

Keywords

Defect taxonomy, Defect Classification scheme for health software, Validation, Taxonomy based testing

1. *Introduction*

Medical devices increasingly rely on software to provide functionality [24]. Software complexity and the rapid growth of the software industry make it difficult to control and prevent defects [17]. Due to the introduction of advanced technologies, the medical device software industry is facing massive growth of complex software [24]. This massive growth of medical device software leads to quality risks.

The US Food and Drug Administration (FDA) reports that from 2005 to 2011, 19.4% of medical device recalls were related to software [28]. Another study focused

[1] This document is still under study and subject to change

on recalls of medical devices related to computer-based failures such as software, hardware, inputs, outputs, or battery. This study reported that 2,303,441 recalls out of 12,024,836 were related to software. Software issues accounted for 33.3% of class I recalls, 65.6% of class II recalls and 75.3% of class III recalls [15,31]. The FDA recall process includes specifically identifying software-related recalls in order to improve medical device quality and to ensure patient safety [7].

Software quality assurance (SQA) practices have been integrated into the software development process to find defects and ensure software quality. SQA processes aim to minimize software defects and show that software meets requirements. There are many SQA activities, such as testing and inspections, which can be used to validate software [30]. Research studies suggest that a defect taxonomy is the best way to prevent and control defects [5,8,9]. People use customized or original defect taxonomies in different domains such as the safety critical domain, the business domain, and the telecommunications domain. Before they use defect taxonomies, they validate their defect taxonomies in terms of reliability, efficiency, and completeness.

This study focuses on validating a new defect taxonomy called SW91 [2]. This paper is structured as follows. Section 2 explains what a defect taxonomy is and how industries have used defect taxonomies during software development. Section 3 explains the benefits of using defect classification schemes. Section 4 explains the development of a new defect classification scheme for health software, SW91. Section 5 explains initial steps taken to validate SW91. Section 6 explains a new testing method called “taxonomy based testing” which details how defect categories from a taxonomy can be used in testing. Section 7 outlines plans for future work where taxonomy based testing will be used to validate SW91. Section 8 presents the summary and conclusions.

2. *State of the art – The use of defect taxonomies in industry*

A defect taxonomy is a system of hierarchical categories designed to be a useful aid for reproducibly classifying defects in the software development lifecycle [14]. There are many other terms for defect taxonomy including fault categorization, defect classification, fault classification scheme and bug taxonomy. In this paper, the terms defect taxonomy and defect classification scheme are used interchangeably. This section explains how different industries used various defect classification schemes for a variety of purposes in different phases of the software development lifecycle in order to improve software quality.

In 1998, at the Motorola Corporate Software Centre, the GSM Products Division’s Base Station Systems (GSMBSS) conducted a study on how the ODC scheme can be used to measure the progress of software development [4]. The ODC scheme was applied to an existing project with data collected by Fagan inspection [30]. After a successful feasibility study using the gathered data to verify the suitability of the ODC scheme, the team mapped defect data with minor modifications into the ODC scheme. This study proved that software development progress measurement and process improvement feedback can be produced from the data which was collected using an existing inspection method by adopting the ODC scheme. The authors of this study believed the ODC scheme can easily be applied to enhance software quality and to improve customer satisfaction while developing defect prevention and qualitative process management techniques [4].

In 2004, Lutz and Mikulski [20] published work on the analysis of 199 anomalies from seven spacecraft at the Jet Propulsion Laboratory. The purpose of this study was to improve the safety of future missions. The ODC scheme was selected to classify the post-launch safety critical software anomalies in order to extract the defect signature. The following outcomes were highlighted from this study:

- Training on documentation of anomalies can limit the reoccurrence of anomalies.
- The benefit of maintaining the documentation of system requirements for the operational process has been identified.
- Anomalies' analysis enhances the reusability of knowledge from one system to another.
- When comparing the outcomes from other methods related to operational risk, the anomaly patterns obtained by classifying the anomalies using the ODC scheme provided additional understanding of operational risks.

Finally, the authors of this study stated classifying anomalies lead to understanding the anomalies triggers and contributed to preventing operational anomalies.

Freimut et al. [10] conducted a study at Robert Bosch GmbH in the business unit for Gasoline Systems (GS) and published their work in 2005. Gasoline Systems developed electronic control units for gasoline engines with embedded software as a key component. To overcome the lack of information related to quality assurance and overall system quality at Bosch GS, it was decided to apply quantitative data management techniques in quality assurance strategies. They defined, introduced and validated a customized defect classification scheme to track defects which are involved in software development and process measurement [10]. The following outcomes were obtained after applying a defect classification scheme:

- Defect flow distribution and its outputs were observed.
- Identification of the defects introduced in early stages and identified in later stages.
- Defect data from the case study which identified categories with a high number of defects.
- Providing the measurement outputs to management.

In 2007, Robillard et al. [26] published work detailing the measurable test efficiency in a software product due to changing testing practices. This research was conducted with a team that developed audio software for video games. Two different testing phases, A and B, were used to measure the test efficiency. Phase A used implicit testing practices to record defects. In the second phase, B, an “Easy to follow” scheme was proposed to record the testing practices in order to make developers aware of the type of testing activities involved. A modified ODC scheme was used to record the defects in both testing phases and the following outcomes were observed [26]:

- The distribution of defects for the type of activity conducted in each phase, such as design review, code inspection, and unit test.
- The distribution of defects based on the discovery attributes. Discover attributes indicate who found the defects.
- The distribution of defects based on the activity qualifier attributes. The activity qualifier attribute indicates whether defects were found opportunistically or during planned testing.

- The ODC scheme was selected to get a statistical understanding of software process measurement using both types of testing.

In 2008, the ODC scheme was used in NASA flight projects. The ODC scheme was used as an extension of the COnstructive QUALity Model (COQUALMO) developed by Raymond Madachy and Barry Boehm from the University of Southern California, USA. The ODC COQUALMO model was used for critical NASA flight projects [21]. The ODC scheme was successfully adopted in defect reduction strategies. The ODC COQUALMO model helped in providing a highly detailed view of the defect profiles and their impact on specific risks. The ODC COQUALMO model with automated risk minimization helped to meet the quality goals of NASA's flight projects in a shorter time with fewer resources [21].

In 2010, Li et al. [19] presented an extended and modified defect classification scheme named the Orthogonal Defect Classification scheme for Black-box Defect (ODC-BD) which was created based on the ODC scheme. This empirical study was aimed at helping black-box defect analysers and black-box testers to improve their testing efficiency and analysis. It was proved that the effort for defect analysis was reduced by 15% after applying the ODC-BD. The test efficiency, measured as the number of detected defects per unit time, in the first week, without using the ODC-BD scheme, was 0.075. In the second month, the test efficiency increased to 0.125 using the ODC-BD scheme [19]. This empirical study with 1660 black-box defects is a good example of measuring the black-box testing process with the ODC scheme.

In 2012, Mellegård et al. [23] published their work on developing an effective and systematic software defect classification scheme at Volvo car corporation in Sweden. They developed a software defect classification scheme "the Light-weight Defect Classification scheme (LiDeC)", which complements the IEEE standard classification for software anomalies [12,13]. This study demonstrated the customization of a generic defect classification scheme to classify defects. Adopting a customized defect classification scheme minimized the time required to find defects while helping to characterize the defects. The HP scheme has been used within Hewlett-Packard departments for many different purposes such as root cause analysis and defect presentation [11,25].

In 2014, Nuno Silva and Marco Vieira [27] published their work which demonstrated the importance of domain specific defect classification schemes. They focused on four systems from the aerospace and space industries. They demonstrated the following problems in adopting a generic classification scheme into a safety critical domain:

- There are problems with adopting a generic defect classification scheme without considering the defect propagation effects and the interconnection of defects from different phases of the software development lifecycle.
- Inability to cover all the defects with existing listed defect types, defect triggers and defect impacts.
- Differentiating dimensions to keep the orthogonality of the defects was not easy to achieve.
- Not showing the connection to the quality models.
- There were difficulties getting the necessary level of information related to each defect to map with the defect type, defect trigger or defect impact.
- Difficulties mapping non-functional defects.
- Difficulties mapping the defects to a related standard.

The above points clearly demonstrate the problems in adopting a generic classification scheme into a safety critical domain. This study highlights the need for improved and domain specific defect taxonomies to classify defects.

Since medical device software is often safety critical, the necessity of a domain specific defect classification scheme has been identified and a defect classification scheme is being developed for healthcare software called SW91 [29]. The development of SW91 is explained in Section 4.

This section detailed how different defect classification schemes were used in different industries from 1998 to 2014 and the importance of domain specific defect classification schemes. The next section discusses the benefits of defect classification schemes.

3. *Benefits of defect classification schemes*

Bernd Freimut [11] has detailed various benefits of defect classification schemes including characterization of the defects found, defect prevention, control inspections, evaluate and improve technologies, control testing, plan testing and reduce field defects.

Vallespir et al. [32] stated a defect classification scheme makes it easy to find the injected defects while providing information on phases, activities, and disciplines throughout the software development lifecycle. Robert B. Grady from Hewlett Packard stated that the benefit of classifying defects is to help find the correct quality assurance activity. He stated: “As you categorize the defects, you will uncover a variety of symptoms. A typical first step will be for you to decide to do better or different inspections or tests” [25]. When combining both Vallespir et al. and Robert B. Grady’s statements, injected defects could be identified and classified by a defect classification scheme. Those classified defects will inform the choice of the correct quality assurance activities.

Kelly and Shepard stated a detailed defect classification scheme plays a significant role in understanding the software development process [18]. Defect classification schemes can be created for several different purposes in a software development organization. These include:

1. Making decisions during software development
2. Tracking defects for process improvement
3. Guiding the selection of test cases
4. Analysing research results [18]

Vogel has detailed a procedure for medical device software defect management. “Classification” is the second of eight steps. Vogel’s defect procedure supports the need for defect classification schemes in medical device software development. He stated the importance of classification in medical device software as follows: “the classification is important for later determination on the recommendations and means for verifying any changes made to deal with the defect”. Safety critical domains have utilized defect classification schemes to reduce defects and to improve analysis [21,24,27]. Safety critical domains have a requirement for a unique defect classification scheme tailored to their unique needs [33]. The medical device software industry is such a safety critical domain and hence should have its own domain specific defect classification scheme.

The Association for the Advancement of Medical Instrumentation (AAMI) is developing a defect classification scheme for health software which includes medical device software. Section 4 explains the development of the defect classification scheme for health software called SW91. Prior to the development of SW91, there has been no defect classification scheme specifically developed for use in the medical device software industry. It is hoped that applying a defect classification scheme into the medical device software industry will bring similar benefits observed in Sections 2 and 3.

4. *AAMI and Development of SW91*

AAMI is a non-profit organization founded in 1967 [1]. AAMI is developing a defect classification scheme named “Classification of Defects in Health Software-SW91” as a standard. This work started in 2014 and aims to provide a common language to classify defects and improve software quality in health software including medical device software [29]. SW91 was published in September 2016 for first public comment and again published in April, 2017 for the second round of public comment. It is expected that the final version of SW91 will be published later in 2017. SW91 includes defect categories from planning a system to maintenance and release of a system.

It contains multi-level defect categories such as parent level and bottom level. Each defect category has its own defect code with a unique number. The numbering system followed in SW91 is flexible to allow new categories to be added as necessary under any parent level of defect category. The next section explains how SW91 has been validated to date.

5. *Validation of SW91*

Before starting the validation of SW91, a brief comparison was done among other relevant defect classification schemes such as the ODC scheme, the IEEE Standard Classification for Software Anomalies and the HP scheme. Bernd Freimut analyzed different defect classification schemes based on their structure and their usability [11]. In the literature defect classification schemes were validated for their reliability, ability to perform useful analysis, and efficiency [10,19,20,22]. These terms will be considered in the validation of SW91. In addition to the above terms, the defect coverage of SW91 will also be validated by this research. Our plan has following three different tracks:

1. Mapping defects from databases.
2. Mapping defects from medical device software companies.
3. Taxonomy based testing.

Section 5.1 explains the first track of the validation and explains how SW91 was mapped with open source data. Section 5.2 presents the second track of validation. The third track of validation is a new approach using taxonomy based testing. Section 6 explains how taxonomy based testing has been used in other industries. Section 7 explains future plans to use taxonomy based testing to validate SW91.

5.1 Mapping SW91 with CWE

The CWE is an open source list containing common software weaknesses and their vulnerabilities. CWE Version 2.9 [6] was the latest version available when the mapping was started. CWE Version 2.9 contains 1004 vulnerabilities. This version of CWE has multiple views such as full dictionary view, development view, research view and fault pattern view.

Prior to the mapping, it was necessary to select the appropriate view of vulnerabilities from the CWE. After carefully analysing the multiple views, SW91 was mapped with the cross section view from the CWE. The approach to the mapping and the selection of the cross section view was discussed and finalized with the SW91 development team. The SW91 development team is composed of members from a number of relevant disciplines such as medical device product development, software engineering, software quality, and regulatory policy with members considered to be expert in their field.

The cross section view contains a selection of software weaknesses which represent the range of weaknesses captured in the CWE. These weaknesses include a total of 158 vulnerabilities [6]. From the CWE cross section, out of 158 vulnerabilities, 150 vulnerabilities were successfully mapped with SW91's defect categories. This was a manual one to one mapping. In my initial mapping it was not possible to find a suitable category from SW91 for the following eight vulnerabilities from the CWE cross section:

173: Improper Handling of Alternate Encoding
175: Improper Handling of Mixed Encoding
222: Truncation of Security-relevant Information
434: Unrestricted Upload of File with Dangerous Type
486: Comparison of Classes by Name
502: Deserialization of Untrusted Data
798: Use of Hard-coded Credentials
323: Reusing a Nonce, Key Pair in Encryption

The one to one mapping was reviewed by the SW91 development team who paid particular attention to the eight vulnerabilities that could not be mapped. The team members checked for the possibility of mapping with SW91's existing defect categories and there was a discussion on adding new defect categories and changing the name of a defect category, in order to ensure that all vulnerabilities could be mapped to a suitable defect category.

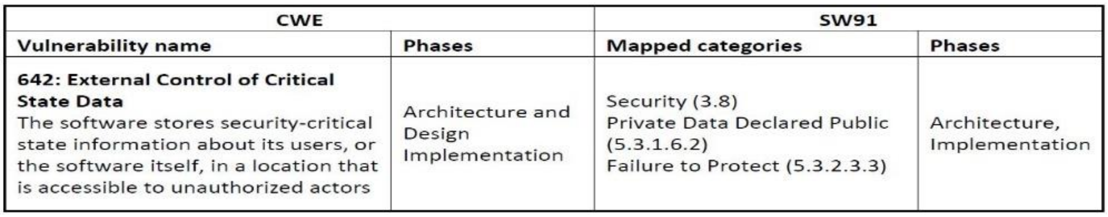
Out of the eight vulnerabilities which could not initially be mapped, five vulnerabilities were mapped with newly added defect categories or defect categories that required name changes. Three vulnerabilities were assigned to an existing defect category. This one to one mapping established that all of the CWE cross section vulnerabilities could be mapped to at least one defect category from SW91.

From the completed one to one mapping, a subset of vulnerabilities was selected by an experienced team member. The selected subset included eighteen vulnerabilities from all phases of the software development life cycle. One to many mapping was conducted for those eighteen vulnerabilities. In one to many mapping, each vulnerability was mapped with possible different defects categories from SW91. The purpose of the one to many mapping was to show the usability of SW9. The initial one to many mappings was conducted by me. Then the SW91 development team reviewed the mapping.

In the validation process out of eighteen mappings, five mappings were accepted by the team without any changes. Three mappings were changed by adding additional defect categories into the existing mapping. Two mappings were changed by adding additional defect categories and deleting some mapped categories. Three mappings were changed by adding additional defect categories including the reason for why those categories were selected. Two mappings were changed by deleting few mapped categories from the mapped defect categories. One mapping was changed by deleting defect category and including the reason for why other categories were selected. Finally two mapping were totally deleted and replaced with new mapped categories.

For example vulnerability 642: External Control of Critical State Data was mapped with the following two categories from SW91 by me. The third defect category was added by the team members when they were validating the one to many mapping:

1. **Failure to Protect (5.3.2.3.3):** Software permits access to an object that should be protected (for security reasons rather than for coherency), assuming the design is correct. **Fehler! Textmarke nicht definiert.**
2. **Private Data Declared Public (5.3.1.6.2):** An object is declared as public when it should be private. The object may be accessible to functions that should not use it, creating an unintended dependency or security vulnerability**.**Fehler! Textmarke nicht definiert.
3. **Security (3.8):** The defects are related to security issues in the architecture, such as compromising of sensitive information, choosing an inappropriate authentication protocol, not using access control, or communication integrity. It may also include the use of unsigned software and the introduction of unknown changes after the software is deployed. Note that many issues related to security involve requirements inadequacies, and many security vulnerabilities might be caused by poor design or implementation activities. Capturing all the causes and contributing factors for a security defect should involve identifying possible Requirement Defects (2.*), Design Defects (4.*) and Implementation Defects (5.*) rather than categorizing every failure associated with security as a Security (3.8) defect. **Fehler! Textmarke nicht definiert.**



CWE		SW91	
Vulnerability name	**Phases**	**Mapped categories**	**Phases**
642: External Control of Critical State Data The software stores security-critical state information about its users, or the software itself, in a location that is accessible to unauthorized actors	Architecture and Design Implementation	Security (3.8) Private Data Declared Public (5.3.1.6.2) Failure to Protect (5.3.2.3.3)	Architecture, Implementation

Figure 1: CWE Mapping**Fehler! Textmarke nicht defi-**

This one to many mapping shows how a user can select multiple different defect categories from SW91 to map to a particular vulnerability. This subset of mappings was added as an annex in SW91. This CWE mapping was conducted as part of the validation of SW91. This work was carried out to determine the defect categories and their coverage in SW91 when compared with publicly available vulnerabilities. This mapping also shows difficulties in reliability mapping data, with different people coming up with different mappings. The next section explains another part of the validation carried out with empirical data from a medical device software development company.[2]

5.2 Mapping SW91 with data from a medical device software company

As a part of the validation process, we contacted a medical device software development company to request empirical data to map with SW91. Company A from Ireland develops medical device software and web-based applications. The benefits of defect classification schemes and the need for a defect classification scheme in the medical device software industry were explained to the management of company A. Data was obtained from company A. The following data has been used in this mapping:

1 Defects
2. Software Design Specification
3. User Requirement Specification (URS)
4. Risks
5. Testing Protocols

The first four data sets were mapped with SW91 defect categories. Figure 2 displays the mappings of data from company A to SW91 defect categories. In mapping A of Figure 2 the defects from company A mapped to nineteen distinct defect categories from SW91. Some slight changes of wording were observed between the defects from the defect data and SW91 defect categories. For example, a defect from the defect data for a “function X” was described as “Units not converting correctly”. This defect was included in the mapping between SW91 defect category and received defect as “Type Conversion” for “function X”.

Then, in mapping B of Figure 2 control flow diagrams from the software design specification document were mapped with eighteen distinct defect categories from SW91. The software design specification document clearly explained the software and the constraints of the system. In addition, control flow diagrams in the software design specification document described the functionality of the system step by step. In this mapping, all elements from the control flow diagrams were mapped into defect categories from architectural defects, design defects, and implementation defects in SW91. Since SW91 uses a hierarchical structure of defects, it was easy to jump into the relevant defect category at the appropriate level. For example, if a control flow diagram has a processing step containing a statement “Count <1”, then searching for a relevant defect category from the implementation defects is straight forward rather than searching for defects from other phases of software development such as requirement defects or maintenance defects. Here the following defect categories were assigned to the above processing step “Count <1”:

- Mixed Sign
- Use Before Check
- Invalid Path
- Operator

The URS document includes forty-two requirements. In mapping C of Figure 2, forty requirements were mapped with thirty-eight distinct defect categories from SW91. Each requirement from the URS document has associated prioritized risks. Despite the URS documents and software design specification documents being prepared for the company’s own use, it was possible to map them with SW91.

A separate mapping of the testing protocols and SW91 defect categories was not performed because the testing protocols are already linked with the software design specification and the user requirements from URS document.

[2] This capture is from the draft version of the standard that was out for public comment.
This is not intended to represent the final version of the standard.

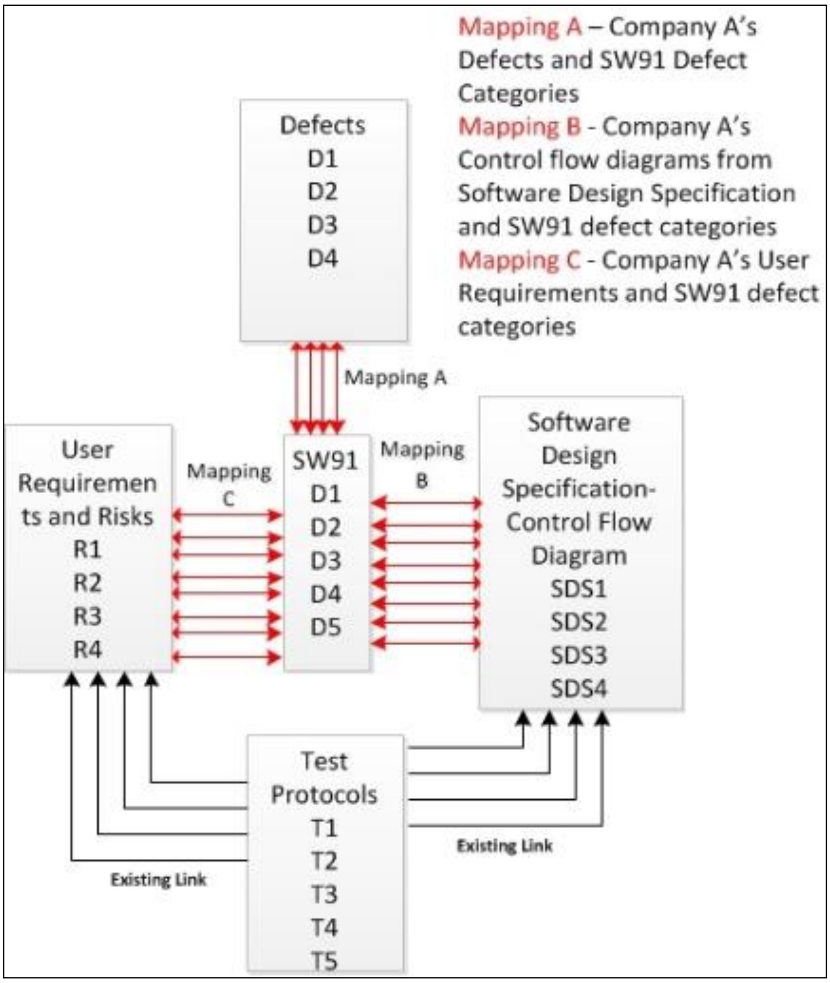

Mapping A – Company A's Defects and SW91 Defect Categories
Mapping B - Company A's Control flow diagrams from Software Design Specification and SW91 defect categories
Mapping C - Company A's User Requirements and SW91 defect categories
Defects
D1
D2
D3
D4
Mapping A
User Requirements and Risks
R1
R2
R3
R4
Mapping C
SW91
D1
D2
D3
D4
D5
Mapping B
Software Design Specification-Control Flow Diagram
SDS1
SDS2
SDS3
SDS4
Test Protocols
T1
T2
T3
T4
T5
Existing Link
Existing Link

Figure 2: Mapping company A's data to SW91

So the defect categories from SW91 were used in both mapping B and C can be directly linked with the respective the testing protocols

From this mapping, five common SW91 defect categories have been identified from all three mappings A, B and C. In this approach, whenever the requirements have been gathered and company A does this mapping, it will enable them to see the possible defect categories for each requirement. This type of mapping also allows goal oriented test cases to be written, consistent with the taxonomy based testing approach. Those goal oriented test cases will be based on the requirements and respective mapped defect categories from SW91. Execution of these goal oriented test cases will save time finding defects when a test case fails. This mapping will improve software quality by identifying defects at an earlier stage of software development such as identified common five defects.Since company A has detailed control flow diagrams, mapping each stage of the control flow diagram with SW91 defect categories will help to minimize defects at the development phase. When we have the anticipated defect categories for every stage, developers can work to avoid those defects. Quality assurance engineers run tests to find the mapped defect categories. This will minimize the time to find the defects and it will help to prevent defects at the earliest possible phase of software development. Company A has risks for every requirement in their URS document. Those risks are prioritized by severity. If every requirement is mapped with defect categories from SW91, the risks can be used to prioritize which defects should be fixed first.

As we discussed in Section 5, in terms of the validation of a defect classification scheme, the reliability of SW91 can be observed here. Normally, the reliability of a defect classification scheme is determined by the mapping of the same defects by different people. If different people map the same defects with the same defect categories from a classification scheme, then it is decided that the defect classification scheme has good reliability. Here, the same defects from three different documents including URS, control flow diagram from software design specification document and defects from defect data mapped to the same categories in SW91. Due to the confidentiality of the data from company A, we are unable to detail all the mappings here. This section explained how an initial empirical validation was carried out with data from a medical device software development company. Future work in this research will use taxonomy based testing as another method of validating SW91. Next section presents an explanation of taxonomy based testing. Section 7 explains plans for future work involving taxonomy based testing.

6. *Taxonomy based testing*

Defect taxonomies can be used in testing [3]. Creating the test cases for the defect categories from a defect taxonomy gives better test coverage [3,15]. Michael Felderer and Armin Beer have conducted significant research on defect taxonomy-supported testing (DTST) [9]. They stated, “Defect taxonomies can be applied to control the design of tests and the quality of releases to keep testing manageable although time and resources in projects are limited”. In their research, a novel process of system testing using a defect taxonomy has been proposed and implemented. A case study was used to explain how a taxonomy can be integrated into the standardized test process defined by the ISTQB. The proposed test process contains five steps. The first four steps of the DTST process were integrated into the first step of the ISTQB test process called “Test Planning and Control”. The next section explains future work with taxonomy based testing.

7. *Future work*

To continue the validation of SW91, our future work will focus on taxonomy based testing in a medical device software development company. This taxonomy based testing will consider the following points in terms of the validation of SW91:

- The efficiency of SW91
- The reliability of SW91
- Useful analyses enabled by SW91
- Defect coverage

Defect data will be requested from medical device software companies. This data will initially be used to check the defect coverage and reliability of SW91. After gathering other necessary data for taxonomy based testing, requirements will be mapped with SW91 defect categories. Test cases will be generated based on those mapped requirements. During the testing process, test cases generated from mapped requirements with SW91 defect categories will be executed and the results will be observed.

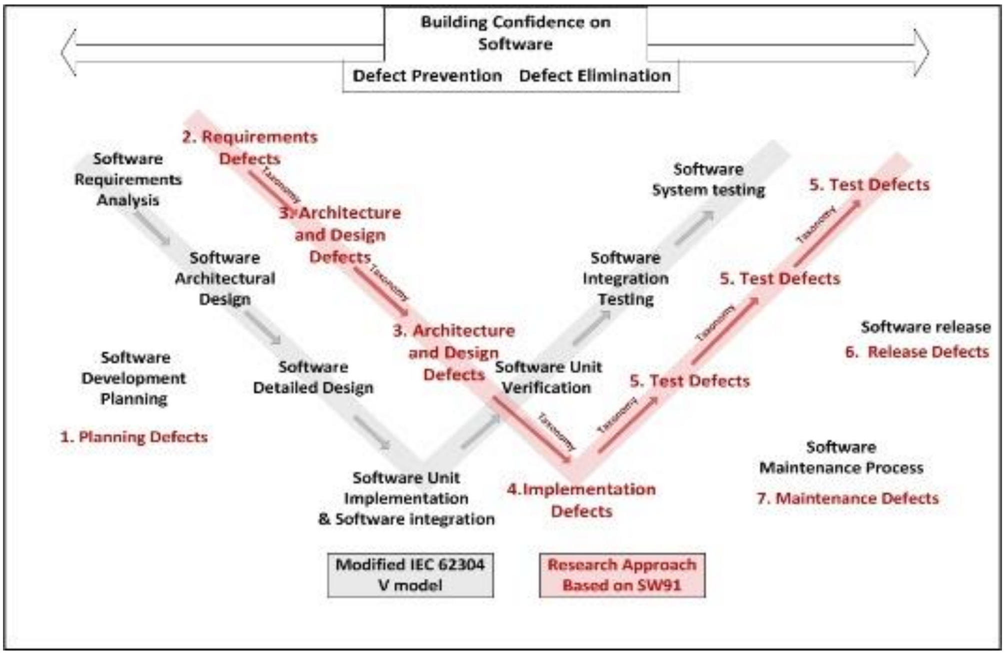

Building Confidence on Software
Defect Prevention
Defect Elimination
Software Requirements Analysis
2. Requirements Defects
Taxonomy
3. Architecture and Design Defects
Software Architectural Design
Taxonomy
3. Architecture and Design Defects
Software Development Planning
1. Planning Defects
Software Detailed Design
Software Unit Implementation & Software integration
Taxonomy
4.Implementation Defects
Software Unit Verification
Taxonomy
5. Test Defects
Software Integration Testing
Taxonomy
5. Test Defects
Software System testing
Taxonomy
5. Test Defects
Software release
6. Release Defects
Software Maintenance Process
7. Maintenance Defects
Modified IEC 62304 V model
Research Approach Based on SW91

Figure 3: Modified IEC 62304 V model and taxonomy based testing

This method of validation will be used to assess the quality of SW91 in terms of efficiency, reliability, performance of useful analyses and defect coverage. Since SW91 includes defect categories for all phases of the software development lifecycle, taxonomy based testing will be used to examine the efficiency of SW91 in finding defects at an earlier stage of the medical device software development lifecycle. When it comes to the reliability of SW91, if a statistically significant number of quality assurance engineers at a medical device software company mapped the same given defects with same defect categories this will demonstrate the reliability. **Fehler! Verweisquelle konnte nicht gefunden werden.** explains the modified V model from IEC 62304 and how SW91 defect categories link with each phase of medical device software development. At the end of the taxonomy based testing, if SW91 helped to increase the test efficiency and helped to reduce similar software defects in future phases, this will be considered as the validation of SW91 in terms of useful analyses. If SW91 covers all identified defects from requirements capture to the final system, this will be considered a validation of defect coverage. Section 8 details the summary and conclusions of this paper.

8. *Summary and Conclusion*

This paper explained software quality problems in medical device software industries and why quality assurance practices may fail to identify defects. The benefits of defect taxonomies were outlined with the empirical examples from the literature. The necessity for a domain specific defect taxonomy in safety critical domains was also explained. The development of a new defect classification for health software (SW91) is underway to address this need in the medical device domain. Validation methods for defect taxonomies from the literature were also presented. As a validation of this newly developed defect classification for health software, two mapping were completed. Firstly, with CWE's vulnerabilities and, secondly, with data from a medical device company. These mappings examined the reliability and the defect coverage of SW91. Finally, our future work will utilize taxonomy based testing to validate the efficiency, reliability, enabling of useful analyses and defect coverage of SW91. Taxonomy based testing will also improve the software quality in medical device software.

9. *ACKNOWLEDGMENTS*

This work was supported with the financial support of the Science Foundation Ireland grant 13/RC/2094 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie).

10. *Literature*

1. Association for the Advancement of Medical Instrumentation. About AAMI. Retrieved 22 December 2016 from http://www.aami.org/membershipcommunity/content.aspx?ItemNumber=1292&navItemNumber=2906
2. Association for the Advancement of Medical Instrumentation. 2016. Classification of Defects in Health Software. 40. Retrieved from http://www.aami.org/standards/downloadables/aamirevf.pdf
3. Rex Black. 2008. *Advanced Software Testing - Vol. 2*. Rocky Nook Inc, Santa Barbara.
4. Norm Bridge and Corinne Miller. 1998. Orthogonal Defect Classification Using Defect Data to Improve Software Development. *Software Quality* 3, 1: 1–8.
5. Ram Chillarege, Inderpal S. Bhandari, Jarir K. Chaar, Michael J. Halliday, Bonnie K. Ray, and Diane S. Moebus. 1992. Orthogonal Defect Classification-A Concept for In-Process Measurements. *IEEE Transactions on Software Engineering* 18, 11: 943–956. https://doi.org/10.1109/32.177364
6. CWE. CWE - CWE-884: CWE Cross-section (2.9). Retrieved 11 January 2017 from https://cwe.mitre.org/data/definitions/884.html
7. FDA. 2014. Medical Device Recall Report FY2003 to FY2012. 1–20.
8. Michael Felderer and Armin Beer. 2013. Using defect taxonomies for requirements validation in industrial projects. In *Requirements Engineering Conference (RE)*, 296–301. https://doi.org/10.1109/RE.2013.6636733
9. Michael Felderer and Armin Beer. 2013. Using defect taxonomies to improve the maturity of the system test process: Results from an industrial case study. In *SWQD 2013*, 125–146. https://doi.org/10.1007/978-3-642-35702-2_9
10. Bernd Freimut, Christian Denger, and Markus Ketterer. 2005. An Industrial Case Study of Implementing and Validating Defect Classification for Process Improvement and Quality Management. In *International Software Metrics Symposium*, 10–19. https://doi.org/10.1109/METRICS.2005.10
11. Bernd Freimut. 2001. *Developing and Using Defect Classification Schemes*. Retrieved from http://en.scientificcommons.org/20203575
12. IEEE-SA Standard Board. 1993. IEEE Standard Classification for Software Anomalies. 32.

13. IEEE-SA Standard Board. 2010. IEEE Standard Classification for Software Anomalies (Revision of IEEE Std 1044- 1993). 15.

14. International Software Testing Qualifications Board. *Standard glossary of terms used in Software Testing*.

15. Ravishankar K. Iyer, Zbigniew Kalbarczyk, Jaishankar Raman, and Jai Raman. 2013. Analysis of safety-critical computer failures in medical devices. *IEEE Security and Privacy Magazine 11*, 14–26. https://doi.org/10.1109/MSP.2013.49

16. Cem Kaner, Jack Falk, and Hung Quoc Nguyen. 1993. Testing Computer Software Second Edition APPENDIX: COMMON SOFTWARE ERRORS. . 1–89.

17. Ali A Karahroudy and M H N Tabrizi. 1996. Software Defect Taxonomy , Analysis and Overview. May.

18. Diane Kelly and Terry Shepard. 2001. A Case Study in the Use of Defect Classification in Inspections. *conference of the Centre for Advanced Studies on Collaborative research*.

19. Ning Li, Zhanhuai Li, and Xiling Sun. 2010. Classification of software defect detected by black-box testing: An empirical study. In *WCSE 2010*, 234–240. https://doi.org/10.1109/WCSE.2010.28

20. Robyn R. Lutz and Ines Carmen Mikulski. 2004. Empirical analysis of safety-critical anomalies during operations. *IEEE Transactions on Software Engineering* 30, 3: 172–180. https://doi.org/10.1109/TSE.2004.1271171

21. Raymond Madachy and Barry Boehm. 2008. *ODC COQUALMO - A Software Defect Introduction and Removal Model using Orthogonal Defect Classification*. Retrieved from http://csse.usc.edu/TECHRPTS/2008/usc-csse-2008-817/usc-csse-2008-817.pdf

22. Marcelo M. Manhães, Maria Claudia P. Emer, and Laudelino C. Bastos. 2014. Classifying Defects in Software Maintenance to Support Decisions Using Hierarchical ODC. *Computer on the Beach*: 283–292.

23. Niklas Mellegård, Miroslaw Staron, and Fredrik Törner. 2012. *A light-weight defect classification scheme for embedded automotive software and its initial evaluation*. https://doi.org/10.1109/ISSRE.2012.15

24. PTC. Software Development for Medical Devices. 1–9. Retrieved 8 April 2016 from https://www.ptc.com/~/media/Files/PDFs/ALM/Integrity/Software_Development_for_Medical_Devices.pdf?la=en

25. Robert B. Grady. 1992. *Practical software metrics for project management and process improvement*. Prentice Hall PTR.

26. P N Robillard and T Francois-Brosseau. 2007. Saying, ‘I Am Testing,’ is Enough to Improve the Product: An Empirical Study. In *ICCGI 2007*, 5. https://doi.org/10.1109/ICCGI.2007.54

27. Nuno Silva and Marco Vieira. 2014. Experience report: Orthogonal classification of safety critical issues. *Proceedings - International Symposium on Software Reliability Engineering, ISSRE*: 156–166. https://doi.org/10.1109/ISSRE.2014.25

28. Lisa K. Simone. 2013. Software-related recalls: An analysis of records. *Biomedical Instrumentation and Technology* 47, 6: 514–522. https://doi.org/10.2345/0899-8205-47.6.514

29. Lisa Simone and Daniel Rubery. 2014. Lisa Simone and Daniel Rubery: A Tower of Babel with Medical Device Software Failures. *AAMIBlog*, 1. Retrieved 24 January 2017 from https://aamiblog.org/2014/10/10/lisa-simone-and-daniel-rubery-a-tower-of-babel-with-medical-device-software-failures/

30. Jeff Tian. 1990. *Software quality engineering*. John Wiley & Sons, Inc, Dallas, TX. https://doi.org/10.1016/0950-5849(90)90039-T

31. U.S. Food and Drug Administration. Recalls, Market Withdrawals, &amp; Safety Alerts - Background and Definitions. Retrieved 3 February 2017 from https://www.fda.gov/Safety/Recalls/ucm165546.htm

32. Diego Vallespir, Fernanda Grazioli, and Juliana Herbert. 2009. A framework to evaluate defect taxonomies. In *XV Argentine Congress of Computer Science*.

11. *Author CVs*

Hamsini Ketheswarasarma Rajaram

Hamsini Ketheswarasarma Rajaram is a Doctoral Researcher in the Regulated Software Research Centre. She graduated with Honors in Bachelor Science in Information Technology (Software Engineering) in the year 2011, at Sheffield Hallam University, UK. She then completed her Master of Science degree in Bioinformatics in 2015, IBMBB University of Colombo, Sri Lanka. Currently, her research focus is on validating medical device software defect taxonomy.

John Loane

Dr. John Loane is a lecturer at the Dundalk Institute of Technology. He is a researcher in the Regulated Software Research Centre and formerly a researcher at the NetwellCASALA research centre. He has received EU FP7 research funding to develop an Indicator-based Interactive Decision Support and Information Exchange Platform for Smart Cities.

Silvana Togneri Mac Mahon

Dr Silvana Togneri Mac Mahon is a Postdoctoral Researcher in the Regulated Software Research Centre. She is currently working as a postdoctoral researcher on a Lero project which focuses on the development of a Medical Device Software Development Framework. She has acted as international project leader, author and editor for the development of ISO/TR 80001-2-7 and is currently involved in the revision of the IEC 80001-1 standard.

Fergal MC Caffery

Dr Fergal Mc Caffery is a Lecturer with Dundalk Institute of Technology. He is the leader of the Regulated Software Research Group in Dundalk Institute of Technology and a member of Lero. He has been awarded Science Foundation Ireland funding through the Stokes Lectureship and Principal Investigator Programmes to research the area of software process improvement for the medical device domain. Additionally, he has received EU FP7 research funding to improve the effectiveness of embedded software development environments for the medical device industry.

A Proposed Model for Software Process Assessment and Improvement in the domain of Global Software Development

Arif Ali Khan1, Jacky Keung1, Mahmood Niazi2, Shahid Hussain1, He Zhang3
1 Department of Computer Science, City University of Hong Kong
{aliakhan2-c@my.cityu.edu.hk,jacky.keung@cityu.edu.hk, shussain7-c@my.cityu.edu.hk}
2Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Saudi Arabia
mkniazi@kfupm.edu.sa
3Software Institute, Nanjing University, China
hezhang@nju.edu.cn

Abstract

Presently, an increasing number of software development organizations are adopting global software development (GSD), mainly because of the significant return on investment it produces. However, GSD is a complex phenomenon, and there are many challenges associated with it, especially those related to software process improvement (SPI). It has been noticed that SPI can a play a significant role in the successful execution of GSD projects. The aim of this research study is to propose a software process improvement implementation and management model (SPIIMM) that can assist SPI practitioners to assess and measure their process improvement readiness prior to SPI implementation in the domain of GSD. SPIIMM will be based on the existing SPI literature, an industrial empirical study with SPI practitioners, and an understanding of the factors that could impact the implementation of SPI initiatives in a GSD environment.

Keywords

Software Process Improvement, Global Software Development, Systematic Literature Review, Success Factors, Barriers, Practices.

1 Introduction

Global software development (GSD) is a relatively recent business strategy for developing high-quality software in low-wage countries at lower cost. In GSD, the software development activities are performed beyond the geographical, cultural and temporal boundaries. The development teams face various challenges due to cultural difference, time difference, language barriers and different social norms and values [1].

The concept of GSD is growing fast and adopted by the majority of software development firms. The main reason behind the acceptance of GSD is the economic factor which is the most motivated tool for software development organizations [2]. Herbsleb [3] reported that business profits, low cost and time, high percent of productivity, access to skillful individuals, innovative concepts and access to market are the benefits which make GSD to be a good choice for the software development organizations.

Besides various benefits, the software quality becomes an enormous issue in the domain of GSD due to the disappointing results of various big projects [4]. Attarzadeh and Ow [5] conducted a survey and they reported that 31.1% of the GSD projects were ended before the completion. The software development firms have recognized that the main challenge of poor software quality is the failure to effectively deploy the software process [6].

Different techniques and methods were introduced to successfully manage the software process among which the prevailing one is software process improvement (SPI). Zahran [7] defined SPI as "the discipline of defining, characterizing, improving and measuring software management, better product innovation, faster cycle time, greater product quality and reduced development costs simultaneously".

Various process improvement models and standards have been designed in order to help software organizations to achieve effective management of software development processes. In particular, capability maturity model integration (CMMI) is one of the process improvement models that consist of organized, systematic and control collection of the best practices for process improvement and assessment [8]. The International Organization for Standardization (ISO) has also developed standards and recommendations for SPI [9]. For example, ISO/IEC 15504 is targeted as process improvement standard under the software process improvement and capability determination (SPICE). SPICE was developed to test and advertise process improvement standards and models [9]. The ISO/IEC 15504 has since evolved into more advance process assessment and improvement standards, such as ISO/IEC 330XX [10]. The ISO/IEC 330XX family covers the assessment of processes deployed in an organization, including their maintenance, change management, delivery, and improvement [10]. Furthermore, the government of the UK has developed an information technology infrastructure library (ITIL) framework in order to support the information technology services [11]. ITIL comprises of best practices to set policies for assessing and improving the information technology related activities by providing the service life cycles [11].

However, slight consideration has been given to develop process improvement models and standards in the context of GSD, which reduce the success rate of SPI programs [12]. It is vital for process improvement practitioners to have deep knowledge of SPI activities in the domain of GSD [12, 13, 14]. Nevertheless, the challenges associated with SPI are quite different in GSD organizations and the practitioners should emphasize on the issues of the process improvement activities in the GSD environment [12]. Niazi et al. [12] highlighted that because of the distributed nature of GSD projects, the implementation of SPI activities is more demanding than collocated environment. The existing SPI literature does not examine the distributed nature of GSD organizations in sufficient details [13-15].

Little attention has been given to conduct empirical studies in order to efficiently execute SPI programs in GSD environments and less attention has been given to develop models and frameworks that could assist the organizations towards the effective implementation of process improvement activities. In this regard, we have proposed a model that could support GSD organizations by providing a robust framework for assessment and improvement of SPI implementation activities. The proposed model could help GSD organizations to effectively manage the process improvement programs.

2 Motivation and Novelty

SPI research is in practice for many years in the areas of information systems and software engineering [12, 16]. Ramasubbu [13] reported that most of the available literature debated process improvement in the context of collocated software development, but currently, a majority of the software firms are adopting the phenomena of GSD. Niazi [17] highlighted that the deployment of SPI activities is a long term approach and required significant time and resources [18]. Even software development organizations committed to provide all the resources do not always accomplish the expected outcomes. Ngwenyama and Nielsen [19] reported the failure rate of SPI programs up to 70% and they mentioned that the root cause of process improvement failure is the limited attention given to the issues associated with the SPI programs.

Richardson et al. [20] argued that in GSD, the team members are physically separate due to the geographical and temporal distances which decrease the direct communication opportunities. Similarly, cultural distance negatively affects the understanding and appreciation level of the activities and efforts of the distributed teams. Process models such as CMM, CMMI and ISO/IEC 15504 operate successfully in a collocated environment, but they do not explicitly address the distributed nature of the software development [20]. A systematic mapping study of SPI in GSD conducted by Kuhrmann et al. [21] reported that existing literature consists of different process improvement proposals and experience reports, but very few studies have discussed standards and models for SPI. They highlighted that the available studies critically discussed the deployment of SPI standards and models like CMMI and ISO/IEC 15504 in the domain of GSD. Presently the distributed software development is extending from focusing only on the cost reduction towards the improvement of all the phases of software development cycle [17].

Ramasubbu [13] reported that the geographically distributed nature of GSD makes challenging to successfully execute the SPI activities. He further discussed that the geographical distribution of the team members brings various other issues related to SPI activities, e.g. to develop practices for process improvement implementation, strategy to shape a strong and positive relationship among the dispersed team members, overcome the time difference and address the cultural challenges. In order to effectively implement these challenges, it is important for the SPI team members to have comprehensive knowledge and understanding of the designing and deployment of process improvement activities [16].

To summarise, despite of the importance of SPI program, no mechanism has been identified in order to competently manage SPI implementation initiatives in distributed environment. There is a pressing need to develop a technique that could help GSD organizations to successfully assess and execute the SPI related activities.

3 Limitations of the Existing Models and Standards

In this section, we have discussed the limitations of existing process improvement models and standards.

3.1 Capability Maturity Model (CMM)

The main objective of CMM is to assess and refine the organizational processes. CMM consists of total five maturity levels (i.e. initial, repeatable, defined, managed, and optimizing) [31]. In CMM maturity levels, level-1 refers to the lowest maturity state of an organization where level 5 refers to the highest maturity level. Each maturity level consists of different key process areas (KPAs). CMM is an effective model for process improvement with defined maturity levels, KPAs and key practices. However, CMM does not provide any information about the effective implementation strategies and deployment of key practices. CMM model does not debated on issues related to humans, such as employee motivation, hiring and selection [22].

3.2 Capability Maturity Model Integration (CMMI)

The structure of CMMI is based on the core components of CMM and the information collected from different other models and real world experiences of organizations that had adopted CMM for years. CMMI also have five maturity levels (i.e. “initial, managed, defined, quantitatively managed and optimizing”) [8]. In comparison to CMM, CMMI gives an innovative view of maturity levels, key practices and the process areas. However, CMMI model does not provide detail information about the implementation of key practices and also does not recommend any implementation strategy [22].

3.3 SPICE (ISO/IEC 15504)

International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC) developed (ISO/IEC 15504) for SPI under the SPICE (Software Process Improvement and Capability determination) program [9]. Process and process capability are the key dimensions of SPICE (ISO/IEC 15504) [7]. The process dimension involves the measurable aim and objective of each process, while capability dimension consists of the attributes of each process [7]. It could be measured using the capability levels. Zahran [7] define capability level as, “a set of attributes that work together to enhance capability to perform a process. Each level provides a major enhancement of capability in the performance of the process”. SPICE integrates the existing process improvement methodologies, but does not provide an explicit process improvement path.

3.4 International Standards Organization (ISO) 9000

ISO 9000 developed a series of standards in order to certify quality systems implemented in firms [32]. These standards could be used to assess the quality of the systems in an organization irrespective to the size and type of the organization or the complexity of the products or services. ISO 9001 consists of guidelines to implement standard organizational management systems. It would assist organizations to fulfil the customer needs and any other involved parties based on the quality management principles presented by ISO. It provides complete guidelines for organizations in order to assess the quality of their management systems [14, 15]. ISO 9001 is a generic standard that mainly focused on manufacturing and services of different types of organizations, instead of just software industry [33]. Similarly, ISO 9001 is a quality management standard and didn’t explicitly explore the process improvement aspects of software systems.

3.5 Implementation Maturity Model (IMM)

Niazi [22] developed a maturity model to assist the process improvement practitioners in order to effectively manage the SPI activities. IMM was based on the key concepts of CMMI [8]. The structure of IMM consists of three core components (i.e. factors, assessment, and implementation). IMM provides the detail information about the deployment of key practices and recommend implementation strategies. The humans related aspects of SPI implementation are explicitly discussed in IMM. However, IMM does not differentiate the collocated and distributed nature of the software development organizations.

4 Research Contribution and Research Questions

A brief survey of literature clarifies that there is a need of framework or model that can contribute to the effective implementation of process improvement in GSD environment. The main concern of this study is to experimentally investigate the views and opinions of SPI experts and to come up with a model that can help the GSD industry to successfully assess and implement the SPI program.

The model will be based on process improvement literature, industrial empirical study and assessment case studies. The focus of our study is to fill the research gap between process improvement research and practice in a way that it becomes accessible to both industrial practitioners and researchers.

For this reason, we have developed the following research questions.

RQ1: What are the factors, as identified in the literature and industrial study that could have positive or negative impact on SPI implementation in the GSD environment?

RQ2: What are the key differences between the factors identified in the literature and industrial study?

RQ3: What are the practices to address the identified factors?

RQ4: How can a practically robust software process improvement implementation and management model (SPIIMM) be developed?

5 Research Methodology

The selected research methods consist of systematic literature review (SLR), survey questionnaire and case study.

- In the first stage, SLR approach will be used to extract the success factors, barriers and implementation practices from the available literature.

- In the second phase, survey questionnaire will be used to empirically assess the findings of SLR and collect additional success factors, barriers and practices apart from the identified ones.
- Develop SPIIMM based on the findings of the SLR and empirical study (survey questionnaire).
- In the last phase, the effectiveness of SPIIMM will be assessed using the case studies conducted in GSD organizations.

The complete research process is presented in Figure 1.

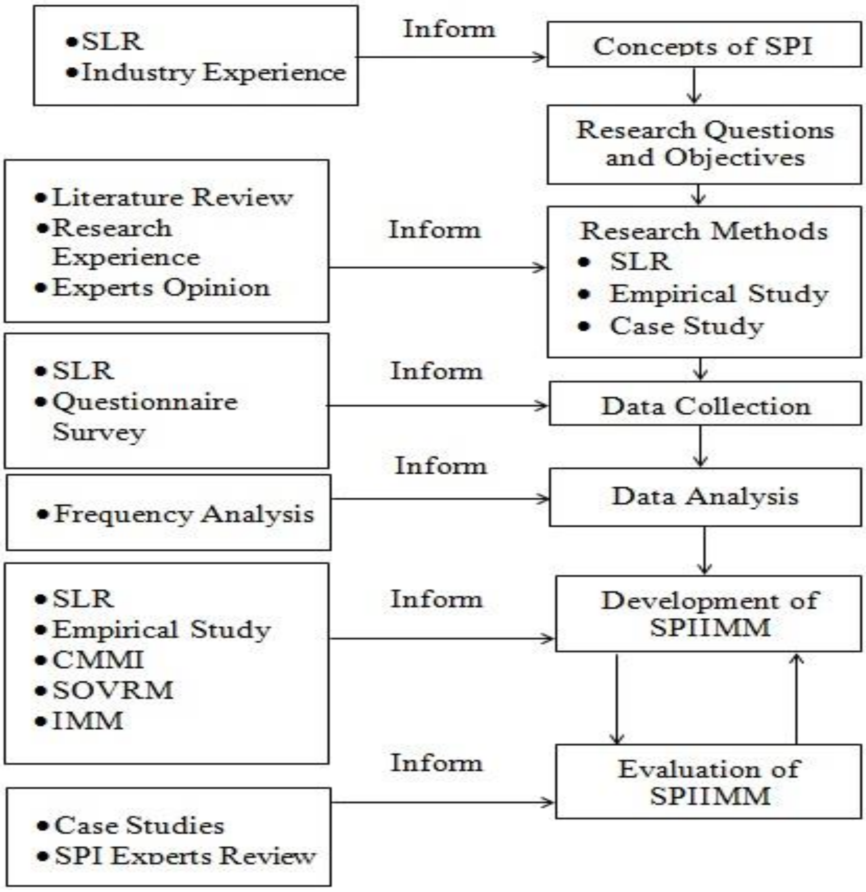


Fig. 1. Research Process.

5.1 Data Collection

We have selected SLR and questionnaire survey techniques to collect the data from existing literature and practitioners. The selected research techniques are chosen because these methods are considered to be suitable for the type of the data involved in this research [22, 23].

Systematic Literature Review. Kitchenham et al. [24] define systematic literature review (SLR) as the methodical way of mining, analysing and reporting the findings of the existing literature associated with any research field and questions of interest. The aim of this SLR study is to analyse maximum relevant available literature by using the step by step instructions of the SLR technique [24]. SLR consists of three core phases i.e. planning the review, conducting the review and reporting the findings of the review

[24]. All the three phases of SLR are briefly discussed in our previous articles [14, 15, 34].

Empirical Data Collection. Bryman [25] discussed that selection of the empirical research methods should be based on the nature of the required data and information, the available resources and the capability of manipulating the variables of interest.
Based on SLR findings, we will develop an online survey questionnaire to investigate the success factors, barriers and practices of SPI in the context of GSD. Questionnaire survey could assist to collect large amounts of data and information from a large group of people “target population” [1]. As the context of this empirical study is GSD, therefore we need to collect the data from a diverse range of process improvement experts working in the domain of GSD across the world. Using survey approach, it is easy to obtain information regarding the attitude of the people. It is difficult to collect such information using observational practices [1].

5.2 Conducting the review

We will use the frequency data analysis technique to analyse the questionnaire survey data and conduct the case studies to evaluate the proposed model (SPIIMM).

Frequency Analysis. Khan [23] reported that frequency analysis is useful for comparative analysis between different variable groups. Frequency analysis could be used to analyse the ordinal, numeric and nominal types of data. In this study, we will follow the frequency analysis in order to calculate the occurrences and comparative analysis of the identified success factors and barriers. The comparative analysis of the identified factors will calculate the relative significance of each success factor. In the same way, the comparative analysis of the identified barriers will highlight the relative importance of each barrier.

Case Study Analysis. Case study approach will be used in order to evaluate the effectiveness of the proposed model (SPIIMM). Case study technique is considered to be the most influential evaluation technique and could provide adequate information about the real world industry experiences [26]. As SPIIMM is designed to implement in the real world software industry, therefore the case study approach is considered to be more suitable and effective for this research study.

6 Structure of Proposed Model (SPIIMM)

The success factors, barriers and practices identified during SLR and empirical study will be used to develop the core components of the proposed model. The identified success factors, barriers and their practices will be structured by following the concepts of the available models, i.e. CMMI [8], IMM [22] and SOVRM [23] in order to develop SPIIMM as shown in Figure 2.
Figure 2 shows the relationship between different components of SPIIMM. It demonstrates that how the findings of the SLR and empirical study assist to develop the core three components of SPIIMM i.e.

- SPIIMM maturity level component
- SPIIMM critical success factors (CSFs) and critical barriers (CBs) component

- SPIIMM practices component

6.1 SPIIMM maturity level component

In this research study, staged representation of CMMI [8] will be followed in order to structure the maturity levels of SPIIMM. It is important to make several adjustments in the structure of CMMI in order to consider its process improvement implementation characteristics.

6.2 SPIIMM factors (CSFs and CBs) component

The five maturity levels of CMMI consist of various process areas (PAs). According to Niazi et al. [27] the maturity levels of SPI could consider in terms of CSFs and CBs rather than process areas. The same concept of using CSFs and CBs has been adopted by different other researchers [27, 28]. They have used CSFs and CBs rather than CMMI PAs. Different researchers have highlighted the significance of CSFs and CBs [27, 29]. Therefore the concept of using CSFs and CBs could be effective to develop SPIIMM.

6.3 SPIIMM practices component

Using the SLR and empirical study approach, different practices will be identified in order to address the CSFs and CBs of factors component. The practices identified during the SLR study will be empirically evaluated and identify additional practices from the SPI experts using the survey questionnaire technique.

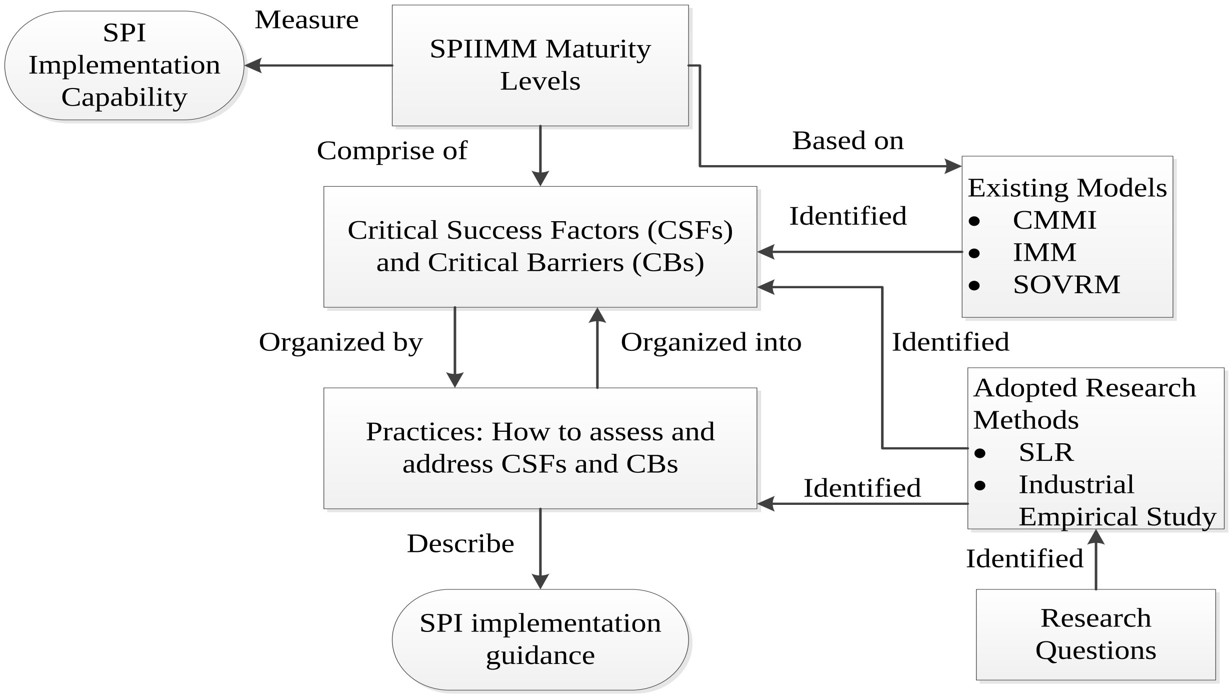


Fig. 2. Architecture of SPIIMM.

7 SPIIMM Assessment Dimension

We have adopted Motorola assessment tool [30] in order to evaluate SPIIMM as shown in Appendix 1. The Motorola assessment tool has been used by different other researchers in order to evaluate their proposed maturity models [23, 27, 28]. The Motorola assessment instrument has been selected due to various compelling reasons. It is normative and has been used and tested at Motorola. It could indicate the weak areas of an organization that need further consideration and improvement [30]. It consists of the following three evaluation dimensions (Appendix 1).

- Approach: This dimension focus on the commitment and support of the organizational management for the practice also the capability of an organization to deploy the practice.
- Deployment: The criterion of this dimension is the consistent and uniform implementation of practice across all the project areas.
- Results: In this dimension the criterion is about the breadth and consistency of positive results over time and across the project areas.

8 Assessment Criteria of SPIIMM

We have selected the following criteria in order to conduct the feedback session with the case studies participants:

- Ease of use: The key objective of this criterion is to assess that how easily the GSD organization can understand and adopt the proposed model (SPIIMM).
- User satisfaction: The SPIIMM should fulfil the requirements of end users and they need to be satisfied with its results.

- Structure of SPIIMM: This criterion is developed to analyse the core components of SPIIMM. It also overview the classification of the reported CSFs and CBs across the maturity levels of SPIIMM.

The assessment criteria are based on the studies conducted by other researchers in different other domains [23, 26-28]. The selected criteria could assess the quality and effectiveness of the product and could help to highlight those areas which contain any deficits and need further improvements [23].

9 Progress up to-date

We have made the following research so far:

- Thorough overview of the literature to identify the research problem.
- Develop the research questions and objectives.
- Finalizing the complete research process.
- Research methods selection.
- Develop the proposed structure of SPIIMM based on the existing models.
- Selection of assessment criteria for SPIIMM.

We have completed the SLR study and launched the second phase of the data collection i.e., industrial empirical study. We have designed and developed the core components of survey questionnaire used to conduct the industrial study. We have done the pilot survey study and till date some interesting results are identified. The results consist of success factors and barriers which are published in our previously published articles [14, 15, 34].

10 Acknowledgment

This work is supported in part by the General Research Fund of the Research Grants Council of Hong Kong (No. 9042328), and the research funds of City University of Hong Kong (No. 7004683 and 7004474).

11 References

1. Khan, A. A., Basri, S., Dominic, P.D.D.: A Proposed Framework for Communication Risks during RCM in GSD. Procedia - Social and Behavioral Sciences, 496-503 (2014)
2. Conchuir, O. E., H. Olsson, P. Agerfalk, Fitzgerald, B.: Benefits of global software development: exploring the unexplored. Software Process: Improvement and Practice, 14 (5), 201-212 (2009).
3. Herbsleb, J. D.: Global Software Engineering: The Future of Socio-technical Coordination. Proceeding of the international conference on Future of Software Engineering., 188-198 (2007)
4. Carmel, E., Espinosa, J. A. and Dubinsky, Y.: Follow the Sun" Workflow in Global Software Development. Management Information Systems, 27 (1), 17-38 (2010)
5. Attarzadeh, I. and Ow, H. S.: Project management practices: the criteria for success or failure. Communications of the IBIMA, (1), 234-241 (2008)..
6. Unterkalmsteiner, M., Gorschek, T., Islam, M.A., Cheng, K. C., Permadi, B. R. and Feldt, R.: Evaluation and measurement of software process improvement—A systematic literature review. IEEE Transactions on Software Engineering, (38), 398-424 (2012).
7. Zahran, S.: Software process improvement: practical guidelines for business success. Journal of Software Maintenance: Research and Practice, vol. 11, 285-291 (1999)

8. SEI.: CMMI® for Development, Version 1.3 (CMU/SEI-2010-TR-033, ESC-TR-2010-033), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, (2010)
9. ISO.: ISO/IEC 15504-4. Information technology- Process Assessment - Part 4: Guidance on use for process improvement and process capability determination. International Organization for Standardization, (2004).
10. ISO.: ISO/IEC 33001. Information technology – Process assessment – Concepts and terminology. International Organization for Standardisation: Geneva, Switzerland (2015).
11. Cartlidge, A., Rudd, C., Smith, M., Wigzel, P., Rance, S., Shaw, S., Wright, T. An Introductory Overview of ITIL® 2011. London: The Stationery Office, (2012).
12. Niazi, M., Babar, M. A., Verner, J. M.: Software Process Improvement barriers: A cross-cultural comparison. Information and Software Technology (52). 1204-1216 (2010)
13. Ramasubbu, N.: Governing Software Process Improvements in Globally Distributed Product Development. IEEE Transactions on Software Engineering (40). 235-250 (2014)
14. Khan, A.A., Keung, J.: Systematic Review of success factors and barriers for Software Process Improvement in Global Software Development. IET Software, 10(5), 125-135 (2016)
15. Khan, A. A., Keung, J., Niazi, M., Hussain, S., Ahmad, A.: Systematic Literature Review and Empirical investigation of Barriers for Software Process Improvement in Global Software Development: Client-Vendor Perspective. Information and Software Technology, (87), 180-205 (2017)
16. Bayona, S., Calvo-Manzano, J. A. and San Feliu, T.: Review of Critical Success Factors Related to People in Software Process Improvement. Systems. Software and Services Process Improvement. Springer Berlin Heidelberg, Germany. 179-189 (2013).
17. Niazi, M.: A comparative study of software process improvement implementation success factors. Software: Evolution and Process 27(9). 700-722 (2015)
18. Khan, A. A., Basri, S., Dominic, P. D. D. and Amin, F.E.: Communication Risks and Best Practices in Global Software Development during Requirements Change Management: A Systematic Literature Review Protocol. Applied Sciences, Engineering and Technology (6). 3514-3519 (2013)
19. Ngwenyama, O. and Nielsen, P. A. 2003.Competing values in software process improvement: an assumption analysis of CMM from an organizational culture perspective. IEEE Transactions on Engineering Management (50). 100-112.
20. Richardson, I., Casey, V., Burton, J., McCaffery, F.: Global software engineering: A software process approach. Collaborative Software Engineering, Springer Berlin Heidelberg, 35-56 (2010)
21. Kuhrmann, M., Diebold, P., Munch, J., Tell, P.: How does software process improvement address global software engineering. IEEE International Conference on Global Software Engineering, 89-98 (2016)
22. Niazi, M.: A Framework for Assisting the Design of Effective Software Process Improvement Implementation Strategies, PhD thesis, University of Technology Sydney, (2004)
23. Khan, S. U.: Software outsourcing vendors' readiness model (SOVRM), PhD thesis, Keele University, UK (2011)
24. Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., Linkman, S.: Systematic literature reviews in software engineering–A systematic literature review. Information and Software Technology (51). 7-15 (2009)
25. Bryman, A.: Social research methods. Oxford University Press, Oxford, (2012)
26. Yin, K. R.: Case study research: Design and methods. Sage publications (2013)
27. Niazi, M., Wilson, D. and Zowghi, D.: A maturity model for the implementation of software process improvement: an empirical study. Journal of systems and software. (74). 155-172 (2005)
28. Ali, S. and Khan, S.U.: Software outsourcing partnership model: An evaluation framework for vendor organizations. Journal of Systems and Software (117). 402-425 (2016)
29. Khandelwal, V. and Ferguson, J.: Critical success factors and the growth of IT in selected geographic regions. 32nd Hawaii International Conference on System Sciences, (1999)

30. Daskalantonakis, M. K.: Achieving higher SEI levels, IEEE Software 11 (4). 17-24 (1994)
31. Paulk, M., Curtis, B., Chrissis, B.M., Weber, C.: Capability Maturity Model for software, Version 1.1. CMU/SEI-93-TR-24, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, (1993)
32. ISO.: ISO 9000. Quality management systems-Fundamentals and vocabulary. Technical Report ISO 9000:2005, International Organization for Standardization, (2005)
33. Chrissis, M.B., Konrad, M. and Shrum, S.: CMMI: Guidelines for Process Integration and Product Improvement, Addison Wesley, Boston, (2003)
34. Khan, A. A., Keung, J., Niazi, M., Hussain, S.: Towards a Hypothetical Framework of Humans Related Success Factors for Process Improvement in Global Software Development: Systematic Review, Proceeding of the 32nd ACM Symposium on Applied Computing (SAC), Morocco, doi: 10.1145/3019612.3019685 (2017)

Appendix: 1

Table 1. Motorola Assessment Instrument [30]

Score	**Key Activity evaluation dimensions**		
	Approach (Score Range: 0, 2, 4, 6, 8, 10)	**Deployment** (Score Range: 0, 2, 4, 6, 8, 10)	**Results** (Score Range: 0, 2, 4, 6, 8, 10)
Poor (0)	• No management recognition of need • No organizational ability • No organizational commitment • Practice not evident	• No part of the organization uses the practice • No part of the organization shows interest	• Ineffective
Weak (2)	• Management begins to recognize need • Support items for the practice start to be created • A few parts of organization are able to implement the practice	• Fragmented use • Inconsistent use • Deployed in some parts of the organization • Limited to monitoring/verification of use	• Spotty results • Inconsistent results • Some evidence of effectiveness for some parts of the organization
Fair (4)	• Wide but not complete commitment by management • Road map for practice implementation defined • Several supporting items for the practice in place	• Less fragmented use • Some consistency in use • Deployed in some major parts of the organization • Monitoring/verification of use for several parts of the organization	• Consistent and positive results for several parts of the organization • Inconsistent results for other parts of the organization
Marginally	• Some	• Deployed in some parts	• Positive measurable results in most parts

qualified (6)	management commitment; some management becomes proactive • Practice implementation well under way across parts of the organization • Supporting items in place	of the organization • Mostly consistent use across many parts of the organization • Monitoring/verification of use for many parts of the organization	of the organization • Consistently positive results over time across many parts of the organization
Qualified (8)	• Total management commitment • Majority of management is proactive • Practice established as an integral part of the process • Supporting items encourage and facilitate the use of practice	• Deployed in almost all parts of the organization • Consistent use across almost all parts of the organization • Monitoring/verification of use for almost all parts of the organization	• Positive measurable results in almost all parts of the organization • Consistently positive results over time across almost all parts of the organization
Outstandin g (10)	• Management provides zealous leadership and commitment • Organizational excellence in the practice recognized even outside the company	• Pervasive and consistent deployed across all parts of the organization • Consistent use over time across all parts of the organization • Monitoring/verification for all parts of the organization	• Requirements exceeded • Consistently world-class results • Counsel sought by others

Autonomous Vehicles?
The Social Aspect? The Ostravian View? An Irish View?

Mícheál Mac an Airchinnigh
Email: mmaa@iscn.com

Abstract

Functional Safety is always a featured topic of the EuroSPI conferences? Hence it seems to be a given to consider all those related technical aspects. In our current culture the car seems to reign supreme. The car is now endowed with all sorts of technologies such as the breaking system, the air bag, and the seat belt, which have been designed and tested. To these we must now add the cybersecurity. There is also a cultural aspect to the car, the shape and look. Once, cars were basically functional. Now they (all) have a certain well-designed aesthetic. But there is another foundational aspect to this: the formal method of design, of shape. [For cyclists, bikers, etc., there are corresponding function design concerns.]

Keywords

aesthetic, brexit, cybersecurity, socialble, testable, Wikipedia

1 Introduction

In an article posted by Richard Messnarz on LinkedIn, December 2016 @11:34 AM, related to the conference, he proposed 7 Key Questions for leading the future in engineering EuroSPI 2017 will offer key discussions with lead industry.

1. Is Agile and Lean possible in a safety driven development? My chosen resource is:

SAFe Scaled Agile http://www.scaledagileframework.com

http://www.scaledagileframework.com/blog/

2. Can Safety and *Cybersecurity* be applied in an integrated approach? Fortunately, the USA Presidential Election 2016 provided an unforgettable experience! One key source is that of *Homeland Security*; https://www.dhs.gov/topic/cybersecurity-education-career-development. “Cybersecurity of automobiles doesn’t just involve the production but also the discovery, proactive measures and patching of vulnerabilities.[43] In 2016 Tesla pushed out security fixes “over the air” and into its cars’ computer systems after a Chinese whitehat hacking group disclosed it with an apparent

altruistic and/or reputation incentive.[44] " (Wikipedia C-class).

3. What new standards are coming out and how do they influence our work? Specifically, are not these new standards European? Now that Brexit is a reality, how shall we communicate/collaborate with the United Kingdom?, for example?

4. How does innovation implementation look like in the future, in a networked and gaming society? Everybody loves to play! Games are fundamentally about playing? Naturally everybody in every culture likes/needs/wants to play! How shall our gamers adopt to the new reality? Specifically, what are the new gaming strategies? Where will they come from?

5. In a world with growing diversity, how can we get teamwork, cooperation and innovation working? Naturally, as usual, it is a person problem! It is a human problem! In every situation there will be conflict, struggle, diametric views! Naturally, a solution will evolve! Unfortunately, the majority may be in the wrong! Many great industries have succumbed! Let us play a game? Name five over the last 10 years?
6. How does the future "Internet of Things" based development and production in industry 4.0 look like? Let us focus specifically on Ostrava? What has been the impact on their society so far? We know of the great Industrial background. But we are also aware of the potential collapse of the current British industrial Complex that is ongoing in the context of Brexit.

7. How can we use trace-ability as a pattern to get the complex systems still connected and understandable?
It is a matter of language! Here we know that the pattern is at the heart of everything! All of Computer science and Mathematics has homed into the essential reality!

8. Ultimately, there is a foundation, a basis, a mathematical one, and it is wedded to the praxis and theory! This was already known in ancient times …

9. Language is of course, diverse as is natural, "see garden of Eden storey" and extrapolate from that! One might imagine that there is a focusing! In a certain reality, with respect to those who speak in their personal linguistic historical tongue!

In a Journal article (The Guardian | Friday 16 December 2016) John Harris proposed the topic : „Why the driverless future could turn into a nightmare" : „The auto revolution is no longer a sci-fi dream – but millions of jobs may go, fuelling yet more alienation." In the Observer (Business) section, UK, "Trains with a guard become driver-only trains, which then become driverless trains." Add in Capita, the UK-based company that runs the London congestion charge; it said it needed to axe 2000 jobs as part of a cost-cutting drive in response to poor trading. It said it would use the money saved from sacking thousands of staff to fund investment in automated technology across all the company's divisions. Uber, the taxi-hailing app was testing driverless cars in San Francisco… It has a deal with Volvo…

„Wages are determined through the antagonistic struggle between capitalist and worker. Victory goes necessarily to the capitalist. The capitalist can live longer without the worker than can the worker without the capitalist. Combination among the capitalists is customary and effective; workers' combination is prohibited and painful in ist consequences for them.“ (Marx 1844).

Adam Smith laid the foundations of classical free market economic theory. *The Wealth of Nations* was a precursor to the modern academic discipline of economics. (Wikipedia). Marx commented that „The ordinary wage... is the lowest compatible with common humanity, that is, with cattle-like exsistence. „The demand for men necessarily governs the production of men, as of every other commodity.“ Now let us reconsider again the driverless car~?

Karl Marx was born at Trier in 1818 of a German-Jewish family converted to Christianity. The author has seen his house. After a failed democratic revolution, he arrived in England as a refugee and lived in London until his death in 1883. It is ironic that today many such people fleeing „Europe“ are stopped at the UK Channel Border.

2 Brexit? Nationalism? Trumpism?

„The decision by Donald Trump's administration to allow internet service providers (ISPs) to sell browsing habits of their customers is „disgusting“ and „appalling“, according to Sir Tim Berners-Lee, creator of the world wide web.“ The Guardian, Wed, 5 April 2017. [WWW launched 1 August 1991]. Berners-Lee also discussed Republican plans to roll back the „net neutrality“ protection that supporters argue is the backbone of an open internet.

In April 2017, Hungary's Parliament has approved a law that may force the famous Central European University to leave Budapest! The Central European University is a graduate-level, English-language university accredited in the U.S. and Hungary and located in Budapest. Wikipedia. (Hungary's Parliament Passes Law Targeting George Soros' University ! April 4, 2017.)

https://www.nytimes.com/2017/04/04/world/europe/hungary-george-soros-university.html?_r=0

Naturally, one might begin by asking what the impact of Brexit will have on “The Global Car Industry”. Instead, it is more prudent/sensible to focus on Europe and in particular Ostrava. The host is VŠB Technical University.

The Technical University of Ostrava (or Vysoká škola báňská – Technická univerzita Ostrava in Czech) is a university (polytechnics) located in the city of Ostrava, Moravian-Silesian Region, Czech Republic.

https://en.wikipedia.org/wiki/Technical_University_of_Ostrava [stub-class article], i.e. “This article has been rated as **Stub-Class** on the project's quality scale. This article has been rated as **Low-importance** on the project's importance scale.” Naturally, there is a good detailed article in Czech :

https://cs.wikipedia.org/wiki/Vysoká_škola_báňská_–_Technická_univerzita_Ostrava

A useful English introduction is available at https://www.vsb.cz/en ; The relevant material is “Computational sciences and information technologies” and “Safety technologies”.

Naturally, one can imagine throwing AQU ; AQUA ; ECTS ; SPICE ; into the mix ? To this we might add Functional Safety; Six Sigma; Integrated approach, et alii.

Suddenly, out of the blue, another crisis emerges: Hungary's Parliament passes a law targeting George Soros's University! April 4, 2017.

https://www.nytimes.com/2017/04/04/world/europe/hungary-george-soros-university.html?_r=0

“The university, known as C.E.U., has been operating in Hungary partly as an American institution and relatively free of Hungarian oversight. But the amended law contains a provision that would most likely restrict the independence of universities that offer diplomas from countries where they do not have a campus or offer courses — a provision that would affect only Central European University.”

https://en.wikipedia.org/wiki/Central_European_University [start-class]

Universities, Institutes of Technology, et allii, are fundamental powerhouses of innovation in all fields. Let us look specifically at some of the consequences ? At this point it is probably a good time to brexit? Naturally, one might begin by asking what the impact of Brexit will have on “The Global Car Industry”.

„Gone are the days when cars made in Britain were British. Yesterday's sale of Vauxhall/Opel to Peugot meant only the transfer of two large English factories from the German subsidiary of an American firm to a French company, accompanied by the ritual promises that jobs would be safe. These seem insubstantial, given that the new management plans to save 1.7bn euro a year from the old Opel operation, while the Vauxhall factories made a heavy loss after the pound's post-referendum slide... Mrs May's industrial strategy might be an intelligent deployment of very limited resources. The future of the car industry is clearly electric, and the development of battery technology – something the government plans to support – will be vital.“ — „The Guardian“ — Published in London and Manchester; March 2017

1. http://jalopnik.com/here-s-how-brexit-could-affect-the-global-car-industry-1782568391

posted by Michael Ballaban.

2. Ford considers UK job cuts after Brexit vote as carmakers eye future (Financial Times)

https://next.ft.com/content/120f17d4-3a17-11e6-a780-b48ed7b6126f

3. NERI Working Paper Series : The Economic Implications of BREXIT for Northern Ireland

Paul Mac Flynn, April 2016
http://www.nerinstitute.net/download/pdf/brexit_wp_250416.pdf

4. „Peugot/Opel : The future of the car industry : will androids dream of electric Jeeps ?“. The Guardian, Number 53,038. 7-03-2017. „Gone are the days when cars made in Britain were British.“ „ ...sale of Vauxhall/Opel to Peugot meant only the transfer of two large English factories from the German subsidary of an American firm to a French company, accompanied by the ritual promises that jobs would be safe.“ But ! The future of the car industry is clearly electric ? The development of

battery technology will be vital", „The Guardian" — Published in London and Manchester;

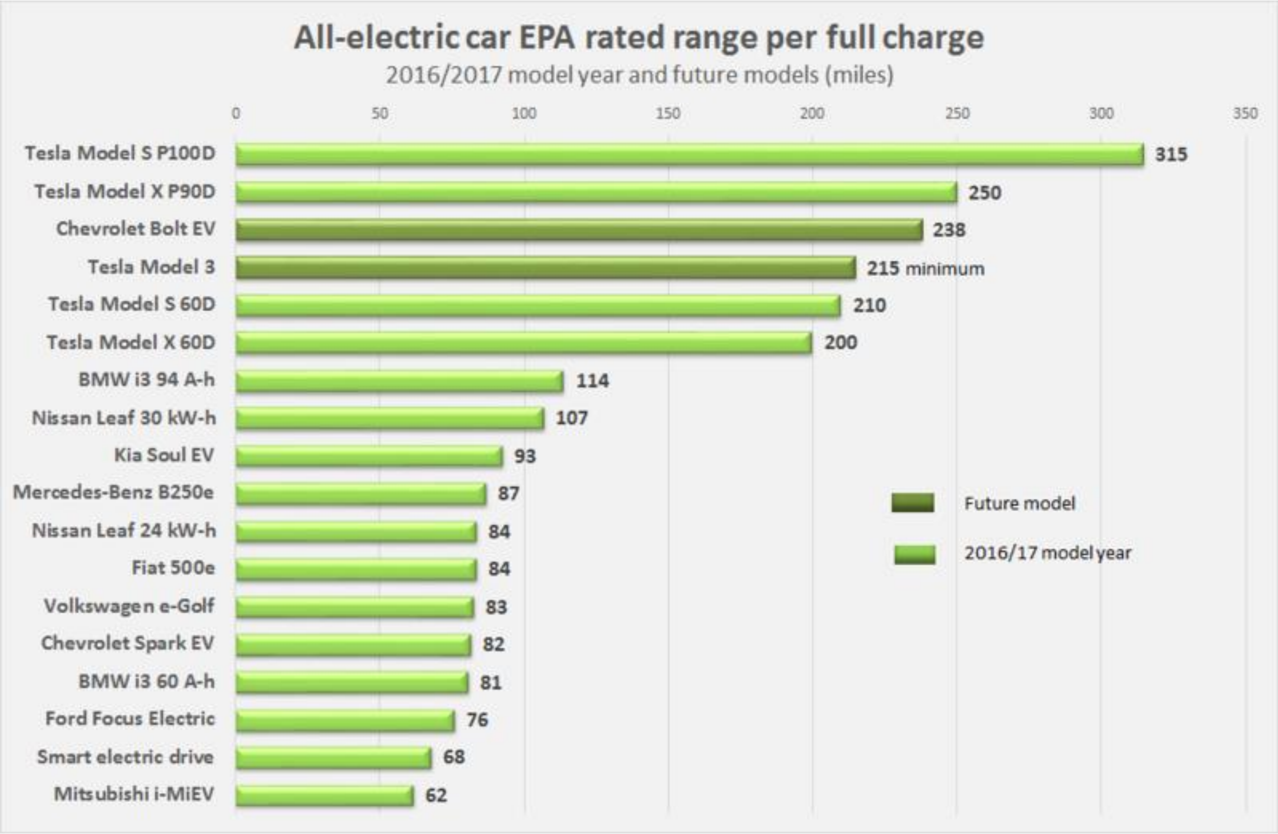
Naturally, one might begin by asking what the impact of Brexit will have on "The Global Car Industry". Instead, it is more prudent/sensible to focus on Europe and in particular the host city of Ostrava.

VŠB – Technical University
The Technical University of Ostrava (or Vysoká škola báňská – Technická univerzita Ostrava in Czech) is a university (polytechnics) located in the city of Ostrava, Moravian-Silesian Region, Czech Republic.
https://en.wikipedia.org/wiki/Technical_University_of_Ostrava

One can expect to find the old familiars: AQU; AQUA; ECTS; SPICE;
Functional Safety; Six Sigma; Integrated approach. What else is there?

Let us consider a particular example of the social side of life?
John Naughton, „The Networker", who writes in the Technical section of the Observer, published a piece under the title of „Why farmers resort to hacking their own tractors." 26.03.17.

3 The John Deere tractor story



John Deere is a large American corporation that makes tractors. „If a farmer bought the tractor he should be able to do whatever he wants with it. You want to replace a transmission and you take it to an independent mechanic — he can put in the new transmission but the tractor can't drive out of the shop." Instead, a Deere technician has to drive to the repair shop and plug a connector into the tractor's USB port in order to „authorise" the new part. The cost : $230 fixed call-out charge, plus $130 an hour on top. --- Farmers have taken to hacking John Deere's software. The cracked software comes mostly from eastern Euro European countries such as Poland.

Legality Issues? Every three years, the US Copyright Office issues exemptions to section 1201 of the Digital Millennium Copyright Act and last October the new list of exemptions included — *mirabile dictu* — tractors ! „The exemption allows modification of „computer programs that are contained in and control the functioning of a motorised land vehicle such as a personal automobile, commercial motor vehicle or mechanised agricultural vehicle", provided that „circumvention is a necessary step undertaken by the authorised owner of the vehicle to allow the diagnosis, repair or lawful modification of a vehicle function". Nebraskan (and other) farmers to hack the embedded software in their tractors as long as they don't tamper with the parts of the programs that control emissions. The response of John Deere is to impose a licence with a clause „You may not reverse engineer, decompile, translate, adapt, or dissemble the licensed materials [i.e. embedded software], nor shall you attempt to create the source from the object code for the software." And if you do, you may be liable for breach of contract... A bird in the Golden Cage syndrome?

4 Formal Methods

The author has spent much of his working life in the field of formal methods, as a member of the computer science department in Trinity College Dublin, Ireland. (see O'Regan, Gerard, 2002). In 1990 the author defined formal software development as

1. a formal specification derived from requirements, and

2. a formal method by which one proceeds from the specification to the ultimate reality of the software.

The specification is written in a mathematical language. In Graz, the author exhibited the power of VDM (Vienna Development Method), a model oriented approach! Today, one ask how might one use formal methods in the contexts of (1) …?

One turns intuitively to Wikipedia to ascertain the current state of the art! Surprisingly, "Formal Methods" is given a "*a start-class article* from Wikipedia, the free encyclopedia"!

Nevertheless it is important to note that "In computer science, specifically software engineering and hardware engineering, **formal methods** are a particular kind of mathematically based techniques for the specification, development and verification of software and hardware systems.[1] The use of formal methods for software and hardware design is motivated by the expectation that, as in other engineering disciplines, performing appropriate mathematical analysis can contribute to the reliability and robustness of a design.[2]

Formal methods are best described as the application of a fairly broad variety of theoretical computer science fundamentals, in particular logic calculi, formal languages, automata theory, and program semantics, but also type systems and algebraic types to problems in software and hardware specification and verification.[3]

It is quite easy to determine the application of Formal Methods, for example, to the automotive industry ! Consider, for example the paper, “Challenges of Applying Formal Methods to Automotive Control Systems”, https://pdfs.semanticscholar.org/4760/005dc493fb994ae7dfe6932141c0ec46a5ee.pdf. Another interesting text is LNCS 8718, Formal Methods for Industrial Critical Systems, 19th International Conference, Florence, Italy, Sept 11-12, 2014.

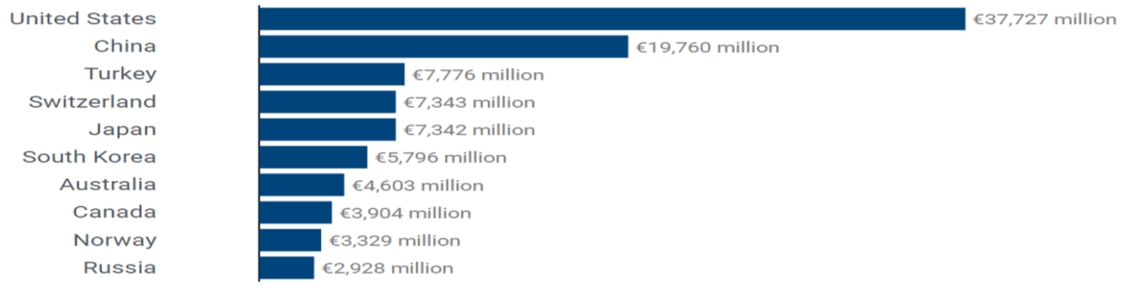
Let us return to the autonomous vehicle ? “An **autonomous car** (also known as a **driverless car**, **auto**,[1] **self-driving car**,[2] **robotic car**[3]) is a vehicle that is capable of sensing its environment and navigating without human input.[4] Many such vehicles are being developed, but as of February 2017 automated cars permitted on public roads are not yet fully autonomous. They all require a human driver at the wheel who is ready at a moment's notice to take control of the vehicle.” Wikipedia. [C-class] For those who are Apple fans, the company has been granted a licence to test autonomous vehicles in California, marking the public launch of its race with Uber, Alphabet, and Tesla”.

5. Social responsibility

“Social responsibility is an ethical framework and suggests that an entity, be it an organization or individual, has an obligation to act for the benefit of society at large. Social responsibility is a duty every individual has to perform so as to maintain a balance between the economy and the ecosystems.” https://en.wikipedia.org/wiki/Social_responsibility [C-class]. One major technological issue in Ireland has been the problem of the water supply ! https://www.water.ie. “Irish Water marks key milestone in Cork Lower Harbour Main Drainage Project.” Unfortunately, there many people in Ireland who have refused to contribute their fair share to the country ! “The European Commission will take infringement proceedings against Ireland due to dangerous levels of chemicals found in drinking water. The commission wrote to the Department of Housing this month confirming that a pilot case it had initiated into the level of trihalomethanes (THMs) in the water system has been closed.” Jan 30 2017. Recently in Dáil Éireann (end of March) it appears that a comprimise might have been reached ! https://www.water.ie/water-supply/supply-and-service-update/ See https://en.wikipedia.org/wiki/Irish_Water [stub-class article].

Corporate social responsibility (**CSR**, also called **corporate conscience**, **corporate citizenship** or **responsible business**)[1] is a form of corporate self-regulation integrated into a business model. https://en.wikipedia.org/wiki/Corporate_social_responsibility [B-class article]. “Some commentators have identified a difference between the Canadian (Montreal school of CSR), the Continental European and the Anglo-Saxon approaches to CSR.[23] It is said that for Chinese consumers,[24] a socially responsible company makes safe, high-quality products; for Germans it provides secure employment; in South Africa it makes a positive contribution to social needs such as health care and education.[25] And even within Europe the discussion about CSR is very heterogeneous.[26]”

The European Automobile Manufacturers Association [ACEA], http://www.acea.be, provide some interesting export figures : Top 10 destinations for EU passenger car exports :



Quick facts:

- The United States remained the EU's most valuable export market for passenger cars in 2016, with exports totalling €38 billion – representing more than 30% of all exports.
- In total, EU passenger car exports fell slightly in 2016 compared to the year before, both in value (-3.2%) and in volume terms (-1.5%); although exports recovered again after the first half of the year, when declines were more significant.
- Throughout the year, car exports generated a trade surplus worth €87 billion for the European Union, down 9.9% compared to 2015.

This data is for quarter 4 2016. One wonders what the data will look like now that Brexit is ongoing?

6. Summing up!

One is already familiar with the Ostrava Experience ? http://whc.unesco.org/en/tentativelists/1560/ [C-class article.] One recalls a similar situation in Wales : “**Ebbw Vale Steelworks** was an integrated steel mill located in Ebbw Vale, South Wales. Developed from 1780, by the late 1930s it had become the largest steel mill in Europe. Nationalised after World War II, as the steel industry changed to bulk handling, iron and steel making was ceased in the 1970s, as the site was redeveloped as a specialised tinplate works. Closed by Corus in 2002, the site is being redeveloped in a joint-partnership between Blaenau Gwent Council and the Welsh Government.”

What does one do to restore confidence in those who are unemployed ? Focusing on the automobile industry in the context of Brexit, it seems that many will feel “disenfranchised” (enfranchise: give the right to vote to…, historically, to free (a slave). See “Enfranchisement referendum (Wikipedia). For example, on 29 November 1995, the President of Poland Lech Wałęsa, after getting permission from Senate, mandated the referendum with the question: Do you approve the enfranchisement of citizens?

To get some sort of picture on the rights of employers and employees (workers) one might refer to the article on Employment : https://en.wikipedia.org/wiki/Employment#Employees_and_employers [C-class article]. The article on the United Kingdom gives some insight : „In the United Kingdom, employment contracts are categorized by the government into the following types:[20]

- Fixed-term contract: last for a certain length of time, are set in advance, end when a specific task is completed, ends when a specific event takes place.
- Full-time or part-time contract: has no defined length of time, can be terminated by either party, is to accomplish a specific task, specified number of hours.[19]
- Agency staff
- Freelancers, Consultants, Contractors
- Zero-hour contracts
- For example, Sports Direct, a retailer, has 90% of its workers on zero-hour contracts[25]
- In August 2013, *The Guardian* reported that J D Wetherspoon, one of the UK's largest pub chains, has 24,000 staff, or 80% of its workforce, on contracts with no guarantee of work each week.[26]
- Hertz Car Rental UK employs workers on a zero-hour contract yearly rather than give guaranteed contracts to save on costs through the winter months. Zero-hour staff are expected to do any evening or weekend work as the full time staff do not want to work these hours.
- Finally, On 2 April 2015, members of the Mandate Trade Union staged a one-day dispute at 109 branches of Dunnes Stores. The dispute concerned low-hour contracts (typically 15 hours per week), income and employment security, and the continued failure of Dunnes Stores to recognise or engage with the Mandate Trade Union, contrary to the recommendations of the impartial Labour Court.[44]

Formal Methods

In 2016, Graz, the author presented some salient aspects of formal methods, choosing in particular a very old one : the Vienna Development Method [VDM] (Dines Bjoerner & Cliff B. Jones 1978). https://en.wikipedia.org/wiki/Vienna_Development_Method The chosen application was the Grocery Shop ! Another formal method, Z, might also have been chosen ! It seems to be right and fitting that it be exhibited this year. **Z** is both a formal language and a specification language. In order to come to grips with Z (if one is a novice) the best way ist o study a simple example : an internal telephone number database ! „The relation between people and their telephone numbers is denoted by :

telephones : Person <–> Phone.
telephones ~ Person X Phone.
Diller gives the example (*diller*, 4794) included in *telephones* ;
This also can be written as diller |—> 4794 included in *telephones* ;
It is possible for one person to have more than one internal telephone (important person) :
Jarrat |—> 4936 included in *telephones* ;
Jarrat |—> 4317 included in *telephones* ;
etc.

A good starting point is, as usual, Wikipedia (to get a simple (?) introduction! https://en.wikipedia.org/wiki/Z_notation [a start-class article]. There is not a lot of practical information! A broader search for Formal specification, leads to https://en.wikipedia.org/wiki/Formal_specification [unassessed!] Another search for Model-based specification https://en.wikipedia.org/wiki/Model-based_specification [unassessed] gives very little information! One suspects that perhaps formal methods are "fading away"? No!

A quick search for Formal Methods Europe http://www.fmeurope.org will quickly reveal the current (European) activities! Of particular interest is the comprehensive document "Formal Methods for Safe and Secure Computers Systems, BSI Study 875, Editor: Dr. Hubert Garavel, Experts: Dr. Hubert Garavel, Dr. Susanne Graf ; Editor: Dr. Hubert Garavel, Experts: Dr. Hubert Garavel, Dr. Susanne Graf.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/formal_methods_study_875/formal_methods_study_875.pdf;jsessionid=55158BFA02E857ED264E69077A1A3A9F.1_cid351?__blob=publicationFile&v=1

7 Literature

Books

1. O'Regan, Gerard, SQC Consulting, A Practical Approach to Software Quality, Springer-Verlag, 2002.
2. Grey, Chris. A very short, fairly interesting and reasonably cheap book about studying organizations. Second Edition. ISBN 978-1-84787-343-9. SAGE. Los Angeles|London|New Delhi|Singapore|Washington DC.
3. Handy, Charles. The Empty Raincoat, Making Sense of the Future. 1994. ISBN 0-09-178022-5.
4. Lacy, Sarah. The Facebook Story, 2009. ISBN 978-1-85458-488-5
5. Marx, Karl. Economic and Philosophic Manuscripts of 1844. Progress Publishers Moscow and Lawrence & Wishart, London. (Comment: NO ISBN available). First published 1959. Translation into English. Progress Publishers 1977.
6. Marx, Karl. Capital Volume I. Penguin Classics. ISBN 0-140-44568-4.
7. Berners-Lee, Tim. Weaving the Web. The Original Design of the World Wide Web, 2000. ISBN 0-06-251587-X.
ISBN 0-387-95321-
3; 80 Upper Friars Rd. Turners Cross, Cork, Ireland; oregang@yahoo.com, http://sqc.netfirms.com, 2002.
Schmidt, Eric and Cohen, Jared. The New Digital Age. 2013. ISBN 978-1-84854-622-6. John Murray (Publishers), 338 Euston Road, London NWI 3BH. www.johnmurray.co.uk (All about Google).
8. Diller, Antoni. An Introduction to Formal Methods. School of Computer Science, University of Birmingham, 1990. ISBN 0-471 92489 X
9. D. Bjorner and C. B. Jones, The Vienna Development Method : The Meta-Language, Springer-Verlag, Berlin, Heidelberg, New York, ISBN 3-540-08766-4, ISBN 0-387-08766-4.

Articles

„Is democracy itself threatened by tech disruption?" Carole Cadwalladr @carolecadwalla. Th e Observer 18.12.16.
„Peugot/Opel : The future of the car industry : will androids dream of electric Jeeps ?". The Guardian, Number 53,038. 7-03-2017. [The Guardian]

Feuer, Eva & Messnarz, Richard & Wittenbrink, Heinz. Experiences with managing social patterns in defined distributed working processes. [Feuer, Messnarz, Wittenbrink] 10-12.12.2003, [2003-12-(10-12)]

Electronic Articles

CyberSecurity
https://en.wikipedia.org/wiki/Computer_security C-class, (a former featured article)
https://www.dhs.gov/topic/cybersecurity-education-career-development
https://www.NERInstitute.net
Social Responsibility
ISO 26000:2010 e-standard
http://asq.org/learn-about-quality/social-responsibility/social-responsibility-in-business.html

Tutorials/Symposia

Messnarz, Richard et al., Integrating Functional Safety, Automotive SPICE and Six Sigma — The AQUA Knowledge Base and Integration Examples. Industrial Proceedings, EuroSPI 2014, June 2 5-27, CRP Henri Tudor, Luxembourg, www.eurospi.net

Messnarz, Richard et al., Implementing Functional Safety Standards. Software Quality Professional. Vol. 17, Issue 3, June 2015.

Industrial Studies

Wikipedia
https://en.wikipedia.org/wiki/Vehicular_automation [start-class]
https://en.wikipedia.org/wiki/ISO_26000 [an unassessed article]

Author CV

Mícheál Mac an Airchinnigh

Prof. Dr. Mícheál Mac an Airchinnigh Emeritus, University of Dublin, Trinity College, Dublin 2, Ireland. 1980-2015. Mathematics, Computer Science, Formal Methods.
President and Founder of ISCN.LTD. 1994
MihalOrela is the *Nom de Plume* of Mícheál Mac an Airchinnigh
with respect to the editing of Wikipedia pages.
Михал Орела is the corresponding Nom de Plume used for Bulgarian Wikipedia.

EuroSPI Blue Book Series

EuroAsiaSPI 2017	VSB – Ostrava, Czech Republic ISBN: 978-3-9504505-0-7
EuroAsiaSPI 2016	Graz University of Technology, Austria ISBN 978-87-9981-1663 (Whitebox, Denmark)
EuroSPI 2015	Ankara University, Turkey ISBN 978-87-9981-1656 (Whitebox, Denmark)
EuroSPI 2014	CRP Henri Tudor, Luxembourg ISBN 978-87-7398-1573 (Delta Improvement Series)
EuroSPI 2013	DKIT, Dundalk, Ireland ISBN 978-87-7398-154-2 (DELTA Improvement Series)
EuroSPI 2012	BENA Center, Vienna, Austria ISBN 978-87-7398-154-2 (DELTA Improvement Series)
EuroSPI 2011	Roskilde University, Denmark ISBN 978-87-7398-153-5 (DELTA Improvement Series)
EuroSPI 2010	Grenoble Institute of Technology, France ISBN 978-87-7398-152-8 (DELTA Improvement Series)
EuroSPI 2009	University of Alcala, Spain ISBN 978-87-7398-151-1 (DELTA Improvement Series)
EuroSPI 2008	Dublin City University, Ireland ISBN 978-87-7398-150-4 (DELTA Improvement Series)
EuroSPI 2007	University of Potsdam, Germany ISBN 978-3-9809145-6-7
EuroSPI 2006	University of Joensuu, Finland ISBN 952-458-864-1, ISSN 1457-9448
EuroSPI 2005	John von Neumann Computer Society, Hungary ISBN 963 8431 94 6
EuroSPI 2004	Norwegian Technical University, Norway TECHNICAL REPORT 07/04, ISSN-NO: 1503-416X
EuroSPI 2003	University of Technology Graz, Austria ISBN 3-901351-84-1

EuroSPI 2002	EuroSPI / ISCN, 2002 ISBN 3-00-010074-1
EuroSPI 2001	University of Limerick, Ireland ISBN 0-9541582-0-2
EuroSPI 2000	Copenhagen Business School, Denmark ISBN 952-9607-29-6
EuroSPI 1999	Pori School of Technology, Finland ISBN 952-9607-29-26, ISSN 1455-9676
EuroSPI 1998	
EuroSPI 1997	
EuroSPI 1996	

The proceedings from 1996 to 1998 have been integrated into an IEEE book: Messnarz, R., Tully, C. (eds.): Better Software Practice for Business Benefit – Principles and Experience, 409 pages. IEEE Computer Society Press, Los Alamitos (1999)

EuroSPI 1995
EuroSPI 1994

EuroSPI 1994 and 1995 proceedings have not been published; exclusive copies are available on request at the EuroSPI office.

-