International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Taguchi's Experimental Design Model Inspired IT Infrastructure Security Risk Assessment Methodology

Erkan Yalcinkaya, Daniel T. Semere, Antonio Maffei, Mauro Onori

Abstract*: *Taguchi's experimental design model is extensively applied by the manufacturing and production industries to systematically simulate different system states through altering controllable and uncontrollable variables to ensure system reliability and robustness. Managing an IT infrastructure complexity in a systematic way to assess the risks is a major challenge. This research paper proposes a novel IT infrastructure security risk assessment methodology inspired by the Taguchi's experimental design model. The proposed methodology is capable of rating and ranking impact of controllable and uncontrollable infrastructure parameters in the form of threats against the system. The result of the assessment is fed into a mitigation process where the system is hardened by eliminating the highest ranking risks.

Keywords*: *Taguchi's experimental design model, cybersecurity, risk assessment, system hardening

I. INTRODUCTION

Most of the contemporary IT systems have become an integrated part of daily life even for an ordinary person. From drinking water to the electricity at homes are distributed with the help of critical infrastructures fully controlled by highly available IT systems which must stand for disruptions in other words they have to be fault tolerant, robust and secure enough to function even during crisis moments. Therefore, assessing and ensuring system security and robustness in a systematic way is paramount important.

Taguchi experimental design is originally proposed to be used to optimize and experiment the quality of manufacturing processes [1]. The flexibility of the design principles allows wide range of applications not only in traditional manufacturing processes but also in other areas such as circuit design [2].

This research paper is devoted to systematically analyze the system security of a reference enterprise IT infrastructure with a methodology adopted from Taguchi's experimental design model.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Erkan Yalcinkaya*, Department of Production Engineering, Royal Institute of Technology, Stockholm, Sweden,E-mail: erkany@kth.se
Daniel T. Semere, Department of Production Engineering, Royal Institute of Technology, Stockholm, Sweden, E-mail: danielts@kth.se
Antonio Maffei, Department of Production Engineering, Royal Institute of Technology, Stockholm, Sweden, E-mail: maffei@kth.se
Mauro Onori, Department of Production Engineering, Royal Institute of Technology, Stockholm, Sweden, E-mail: onori@kth.se

II. TAGUCHI'S EXPERIMENTAL DESIGN MODEL

Taguchi's experimental design model was developed by Genichi Taguchi to experiment on various controllable and uncontrollable parameters to ensure robustness of a product and manufacturing processes during design phase without having to produce the product (versus try and error approach which is costly) [5]. The Taguchi method is widely used in manufacturing industries but other domains such as electronic circuit design also adopts the methodology to design robust products within the specifications [2].

Taguchi's proposed design model comprised of three main phases as follows [5]

- System design
- Parameter design
- Tolerance design

Although all three phases are important to ensure the system robustness and quality, the strength and flexibility of Taguchi's method boils down to the parameter design stage which inputs controllable and uncontrollable system variables affecting the quality of manufacturing process and systemically experiments (i.e. simulates) various combinations to ensure high reliability and robustness.

III. TAGUCHI'S EXPERIMENTAL DESIGN MODEL INSPIRED IT INFRASTRUCTURE SECURITY ANALYSIS METHODOLOGY

IT infrastructure security and robustness depend on number of factors. Therefore, systematic analysis experimenting combinations of different parameters becomes paramount importance to manage the complexity. Taguchi's method outlined in the previous section manages the complexity by systematically experimenting different scenarios by altering parameters. The systematic experiments are performed with the help of orthogonal arrays and the results are considered to design the most robust system.

A similar approach to Taguchi's methodology with the following design stages could be adopted to analyze or determine the IT infrastructure security from the enterprise holistic view.

A. System Design

System design is the initial phase during which the infrastructure elements as well as the assets and the infrastructure topology are identified. By doing so, high-level infrastructure holistic view is achieved, thus all ingress/egress points and component interactions are made visible for further analysis in parameter design phase.

B. Parameter Design in the form of Risk Analysis

Parameter design is the heart of Taguchi's methodology. First, all controllable and uncontrollable parameters are identified and listed. The parameter identification is optionally followed by the parameter prioritization intermediary step if there are too many parameters to consider.

The Taguchi's proposed configuration levels can be treated as the system configuration states in IT terms. These states represent the status of IT infrastructure elements playing major role to determine the system vulnerabilities in relation to the overall architecture.

Potential threats and their likelihood along with estimated impacts are then forming the list of threat landscape. Then the quantitative risk value for each threat is calculated by considering the likelihood and impacts.

The system configuration states versus parameters as experimental runs are combined in the form of an orthogonal array. Because the controlled and uncontrolled parameters are distinct sets, two separate experiment segments are formed. The controlled parameter experiments are named "inner loop matrix" and uncontrolled are named "outer loop matrix" by following Taguchi's terminology.

The inner and outer loop matrices are methodically combined to form the design matrix. Each experiment run represents a system state with bunch of vulnerable configurations and based on the combination of vulnerabilities, a potential security threat is chosen from the threat landscape list.

Finally, the numerical values of probable risks are arithmetically summed up for each experiment. The resulting highest ranked experiment represents the combination of parameters in the form of vulnerabilities posing the highest security risk to the system which can be an input to the system hardening phase described in the following section.

C. System Hardening

The outcome of parameter design identified the highest risk factors. Traditional IT security risk management methodologies suggest several strategies to mitigate the risks. However, this paper focuses only mitigating the risks by applying appropriate security controls to harden the system.

IV. REFERENCE ENTERPRISE IT INFRASTRUCTURE

Modern enterprise IT infrastructures are predominantly known to be extremely complex and consists of numerous elements which can be categorized as follows [3]:

1. *Application layer* consists of the enterprise applications.
2. *Infrastructure management tools and services layer* consists of core IT services such as IAM, directory servers, intrusion detection systems, email gateways and other supporting services and tools to manage the enterprise infrastructure.
3. *Server layer* covers the physical and virtual server instances with operating systems and service layer software and services.
4. *Storage layer* can be considered as the data layer where the application data is logically and physically stored (NAS, SAN file servers, etc.)
5. *Network layer* enables communication among other infrastructure elements. Firewalls, switches, routers, load balancers, Ethernet cables etc. are a few examples.
6. *Facilities layer* consists of infrastructure supporting elements and functions such as power lines, physical space for servers, cooling etc.

Given the list of basic infrastructure elements above, it is now possible to frame a mockup reference enterprise IT infrastructure [4] as illustrated in Figure 1 which will be assessed with the proposed methodology.

The reference IT infrastructure in Figure 1 has three network segments; public internet (uncontrolled), demilitarized zone (DMZ, controlled) and internal network (restricted intranet); separated from each other by external (separating uncontrolled and controlled zones) and internal (separating controlled and restricted zones) firewalls.

In addition to enforcing company security policies, the internal and external firewalls control the ingress and egress traffic to the segmented blocks.

DMZ (controlled) may contain number of servers (email, FTP, internet facing application servers i.e. corporates public web page, API gateways etc.) which are exposed to the external world in other words internet through the enterprise gateway and external firewall.

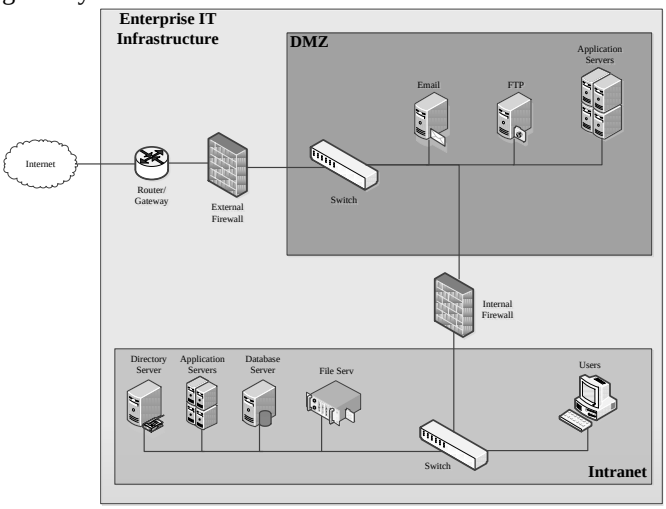

Figure 1 – Reference Enterprise IT Infrastructure components and their interactions

The intranet, inner network segment, contains the rest of the enterprise infrastructure components such as directory servers, database servers, application servers and finally the end user workstations.

The routers or corporate gateways set the enterprise logical boundaries in other words separate the internet and corporate network. Their task is to connect the enterprise infrastructure to the internet and keep address transition tables to convert the corporate local IP addresses to the external public IP addresses or vice versa.The switches connect number of infrastructure elements such as servers, workstations etc. with each other and route packages among those devices so that the enterprise network connectivity is ensured.

V. REFERENCE ENTERPRISE IT INFRASTRUCTURE PARAMETERS IN THE FORM OF VULNERABILITIES

The enterprise IT infrastructure parameters can be categorized as controllable and uncontrollable. The following subdomains identify and categorize the system parameters for the reference enterprise IT infrastructure.

A. Abbreviations and Acronyms

The following table (Table 1) specifies a set of sample system parameters whose state can lead to a weakness or vulnerability for the reference infrastructure outlined in Figure 1. The parameter states are controlled by the system administrator or infrastructure owner.

ID	System parameters in the form of vulnerability or weakness	State	
C_1	OS, enterprise software and firewall configurations, patches and updates	Patched	Un-patched
C_2	Existence of antimalware software such as antivirus, intrusion detection and prevention systems	Yes	No
C_3	Hardware quality	Low	High
C_4	Existence of systematic backup	Yes	No
C_5	Existence of password policy and enforcement	Yes	No
C_6	Existence of network layer encryption	Yes	No
C_7	Server room temperature	High	Low
C_8	Existence of infrastructure monitoring, surveillance and security testing	Yes	No
C_9	Existence of server room access control and physical security	Yes	No
C_{10}	Existence of system and audit logging	Yes	No
C_{11}	Existence of unused/insecure protocols and interfaces in servers	Yes	No

Table 1 – Controllable parameters

B. Uncontrollable parameters

Table 2 specifies number of variables or factors in the form of vulnerability or weakness a long with their states which cannot be directly controlled by the system administrator or infrastructure owner.

ID	System parameters in the form of vulnerability or weakness	State	
UC_1	Unknown (Zero-day) vulnerabilities or special type of weaknesses which are known but impractical to fix	Yes	No
UC_2	Advanced persistent attack	Yes	No
UC_3	Human factor	Yes	No

Table 2 – Uncontrollable parameters

VI. THREATS AGAINST THE REFERENCE ENTERPRISE IT INFRASTRUCTURE

Any contemporary enterprise IT Infrastructure is composed of number of elements many of which are subject to cyber threats. European Network and Information Security Agency (ENISA) annually releases threat landscape reports and ranks the predominant cybersecurity threats. Table 3 as follows is compiled in the light of the information gathered from the ENISA report published for the year 2018 [8] to list the potential security threats against the reference architecture outlined in Figure 1.

ID	Security Threats	Infrastructure Element	Likelihood	Quantitative Likelihood	Impact	Quantitative Risk
D_1	Malware spread	Directory server	Unlikely	2	8	**16**
D_2	Web based attacks	External facing application servers	Possible	3	9	**27**
D_3	Phishing attacks	Users	Likely	4	7	**28**
D_4	Spam campaigns	Email server	Likely	4	7	**28**
D_5	Denial of service	External facing application servers	Possible	3	5	**15**
D_6	Ransomware attack	File server and end user workstations	Possible	3	8	**24**
D_7	Insider threats	Internal facing application servers	Unlikely	2	8	**16**
D_8	Data breach	Database server	Possible	3	10	**30**
D_9	Physical damage/theft/lost	All servers inside the data center	Unlikely	2	8	**16**

Table 3 – Security threats and corresponding risks

Although there are many ways to calculate quantitative risk, this research paper refers to the technique exemplified by [9] which proposes the following risk calculation formula.

$$Risk = Likelihood \times Impact$$

VII. APPLICATION OF TAGUCHI'S PARAMETER DESIGN FOR THE REFERENCE ENTERPRISE IT INFRASTRUCTURE PARAMETERS

The Taguchi's parameter design phase inputs controllable and uncontrollable parameter (specified in Table 1 and Table 2) sets in the form of orthogonal arrays for the analysis. The controllable parameters are aligned in inner loop and uncontrollable parameters are aligned in outer loop of experimental runs [6].

The orthogonal arrays are named as $L_r(n^c)$ for which the

											$UC_1UC_2UC_3$	1	2	2	1	2	1	1	2
											UC_2UC_3	1	2	2	1	1	2	2	1
											UC_1UC_3	1	2	1	2	2	1	2	1
											UC_3	1	2	1	2	1	2	1	2
											UC_1UC_2	1	1	2	2	2	2	1	1
											UC_2	1	1	2	2	1	1	2	2
											UC_1	1	1	1	1	2	2	2	2
											Outer Run	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***
Inner Run	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	***Results***							
1	1	1	1	1	1	1	1	1	1	1	1	D_3	D_3	D_4	D_7	D_1	D_1	D_7	D_9
2	1	1	1	1	1	2	2	2	2	2	2	D_8	D_4	D_8	D_6	D_7	D_5	D_2	D_4
3	1	1	2	2	2	1	1	1	2	2	2	D_2	D_4	D_3	D_6	D_7	D_5	D_8	D_9
4	1	2	1	2	2	1	2	2	1	1	2	D_7	D_1	D_3	D_5	D_6	D_5	D_8	D_1
5	1	2	2	1	2	2	1	2	1	2	1	D_9	D_1	D_8	D_1	D_7	D_8	D_2	D_1
6	1	2	2	2	1	2	2	1	2	1	1	D_1	D_2	D_8	D_9	D_6	D_7	D_2	D_2
7	2	1	2	2	1	1	2	2	1	2	1	D_6	D_2	D_8	D_8	D_7	D_7	D_6	D_6
8	2	1	2	1	2	2	2	1	1	1	2	D_2	D_3	D_9	D_2	D_2	D_2	D_2	D_5
9	2	1	1	2	2	2	1	2	2	1	1	D_4	D_3	D_4	D_9	D_2	D_5	D_2	D_4
10	2	2	2	1	1	1	1	2	2	1	2	D_1	D_1	D_4	D_9	D_2	D_5	D_1	D_1
11	2	2	1	2	1	2	1	1	1	2	2	D_1	D_1	D_6	D_6	D_7	D_6	D_1	D_1
12	2	2	1	1	2	1	2	1	2	2	1	D_1	D_1	D_1	D_1	D_7	D_6	D_1	D_1

Table 6 – Taguchi Design Matrix with inner and outer runs

variable "r" represents the number of experiments, variable "n" indicates the levels of each factor and finally the variable "c" is equal to the total number of factors [7]. The relationship with these variables is formulated with the following equation [6]:

$$r = (n-1) \times c + 1$$

Having applied the formula for the controllable parameters (inner loop) where there are "2" states defined as the number of factors ("n"), and there are "11" controllable parameters listed ("c"), the number of experiments is evaluated as follows:

$$r = (2-1) \times 11 + 1$$
$$r = 12$$

Given the above calculations, Table 4 demonstrates the L_{12} orthogonal array of $L_{12}(2^{11})$ experimental design (saturated i.e. when the number of columns is equal to the number of factors) for the controllable variables.

Exp. Number	***Column***										
	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}
1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	2	2	2	2	2	2
3	1	1	2	2	2	1	1	1	2	2	2
4	1	2	1	2	2	1	2	2	1	1	2
5	1	2	2	1	2	2	1	2	1	2	1
6	1	2	2	2	1	2	2	1	2	1	1
7	2	1	2	2	1	1	2	2	1	2	1
8	2	1	2	1	2	2	2	1	1	1	2
9	2	1	1	2	2	2	1	2	2	1	1
10	2	2	2	1	1	1	1	2	2	1	2
11	2	2	1	2	1	2	1	1	1	2	2
12	2	2	1	1	2	1	2	1	2	2	1

Table 4 – Inner loop matrix, saturated design, L_{12}

The relationship of uncontrollable variables (outer loop) with each other is not exclusive and on the contrary the interactions confounded. For instance, advanced persistent attacks typically exploit careless employees opening an infected email or many unknown zero-day vulnerabilities occur due to time pressured developers focusing only on system functionalities but not security. In such special cases where the variables are correlated, Taguchi suggests applying linear graphs or interaction tables to find out interactions [6]. In the light of these facts and knowing all the factors listed in Table 2 are correlating and interacting with each other, it is suggested to accommodate all interacting combinations in Table 5 with an L_8 array.

Exp. Number	***Column***						
	UC_1	UC_2	UC_1UC_2	UC_3	UC_1UC_3	UC_2UC_3	$UC_1UC_2UC_3$
1	1	1	1	1	1	1	1
2	1	1	1	2	2	2	2
3	1	2	2	1	1	2	2
4	1	2	2	2	2	1	1
5	2	1	2	1	2	1	2
6	2	1	2	2	1	2	1
7	2	2	1	1	2	2	1
8	2	2	1	2	1	1	2

Table 5 – Outer loop matrix, unsaturated design, L_8

By harmonizing Table 4 and Table 5, it is now possible to form the Taguchi's design matrix as shown in Table 6 which combines the inner and outer runs for the reference enterprise IT architecture defined in Figure 1. The heart of the analysis lies under the "Results" table. Each state defined for the controllable and uncontrollable variables listed in Table 1 and 2 yields to vulnerability. After carefully performing qualitative gap analysis against each vulnerability combination, highest probable threats and risks are chosen from Table 3 which at the end structures the "Results" table. It is worth mentioning at the this point that the security threats identified in the "Results" matrix is based on author's own qualitative analysis according to ENISA report findings [8].

VIII. ANALYSIS

This section analyses the experimental design results indicated in Table 6 to identify the most significant risk. The analysis is based on the outcomes framed by the "Results" sub table. To quantitatively rate the risks, the corresponding risks scores from Table 3 are arithmetically accumulated per run and the highest-ranking value represents the highest risk. The suggested analysis methodology only considers the controllable variables because those shall be eligible for system fine-tuning to mitigate the risk.

As shown in Table 7, experiment run number 9 with the highest risk rating score turns out to be the most significant risk.

Run	Results								Risks	∑
1	D_3	D_3	D_4	D_7	D_1	D_1	D_7	D_9	28+28+28+16+16+16+16+16	**164**
2	D_8	D_4	D_8	D_6	D_7	D_5	D_2	D_4	16+28+30+24+16+15+27+28	**184**
3	D_2	D_4	D_3	D_6	D_7	D_5	D_8	D_9	27+28+28+24+16+15+30+16	**184**
4	D_7	D_1	D_3	D_5	D_6	D_5	D_8	D_1	16+16+28+15+24+15+30+16	**160**
5	D_9	D_1	D_8	D_1	D_7	D_8	D_2	D_1	16+16+30+16+16+30+27+16	**167**
6	D_1	D_2	D_8	D_9	D_6	D_7	D_2	D_2	16+27+30+16+24+16+27+27	**183**
7	D_6	D_2	D_8	D_8	D_7	D_7	D_6	D_6	24+27+30+30+16+16+24+24	**191**
8	D_2	D_3	D_9	D_2	D_2	D_2	D_2	D_5	27+28+16+27+27+27+27+15	**194**
9	D_4	D_3	D_4	D_9	D_2	D_5	D_2	D_4	28+28+28+16+27+15+27+28	**197**
10	D_1	D_1	D_4	D_9	D_2	D_5	D_1	D_1	16+16+28+16+27+15+16+16	**150**
11	D_1	D_1	D_6	D_6	D_7	D_6	D_1	D_1	16+16+24+24+16+24+16+16	**152**
12	D_1	D_1	D_1	D_1	D_7	D_6	D_1	D_1	16+16+16+16+16+24+16+16	**136**

Table 7 – Accumulated risks per run

IX. HARDENING THE INFRASTRUCTURE BY MITIGATING THE HIGHEST SECURITY RISK FACTORS

The experiment number 9 simulates the system configuration state where the operating system, enterprise software and firewall configurations, patches and updates are not up to date; systematic backups and network encryption do not exist; password enforcement and password policy are not in place; the monitoring, surveillance systems are not sufficient and security testing practices are not followed; physical access control mechanisms and physical security of server rooms are not in desired level.

The weaknesses mentioned above could be mitigated by fine tuning the controllable infrastructure variables in a desired way. In other words; servers, workstations etc. should be updated with the latest patches; systematic incremental and differential backups should be employed to enable system recovery capabilities during crisis moments; network traffic should be encrypted to ensure confidentiality of data in transit; the enterprise policies should mandate extensive password policies and fine-grained access control mechanisms to ensure accountability; system and network monitoring tools should be deployed enterprise wide; the safeguards and systems should be systematically and regularly tested; last but not least the human and information assets have to be physically protected.

X. FURTHER RESEARCH AREAS

The number of parameters used for assessment may easily become overwhelming even for a mid-sized enterprise infrastructure and performing a threat analysis might not be a trivial task under these circumstances. Therefore, designing and developing a special tool to support the assessment after certain complexity (such as L_{12}) would help to make the method more practical.

XI. CONCLUSION

This research paper focuses on Tagichi's experimental design model which is predominantly used by the manufacturing industry and proposes a novel infrastructure risk assessment and rating methodology inspired by the Taguchi's methodology.

The proposed methodology is first applied to an imaginary small-scale IT infrastructure, then the identified threats against the system are subsequently rated for the right prioritization. The controllable parameter configurations representing the system vulnerabilities are finally fine-tuned to harden the system.

REFERENCES

1. G. Taguchi, "Taguchi methods in LSI fabrication process," in Proc. IEEE Int. Workshop Stat. Methodology, pp. 1–6, 2001.
2. G. Taguchi, S-C. Tsai, "Quality engineering (Taguchi methods) for the development of electronic circuit technology," IEEE Transactions on Reliability, Vol. 44, No. 2, pp. 225–229, 1995
3. C. Longbottom, S. J. Bigelow, "What is IT Infrastructure? Definition from WhatIs.com", [Online]. Available: https://searchdatacenter.techtarget.com/definition/infrastructure [Accessed: 7 - Aug - 2019], 2017
4. M. Endrei, J. Ang, A. Arsanjani, S. Chua, P. Comte, P. Krogdahl, M. Luo, T. Newling, "Patterns: Service Oriented Architecture and Web Services", IBM Redbooks, p 11, 2004
5. J.Z. Zhang, J.C. Chen, E.D. Kirby, "Surface roughness optimization in an end-milling operation using the Taguchi design method", Journal of Material Processing Technology, 184(1-3), pp 233-239, 2007
6. D. T. Semere, "Robust Design Module III", FMG3915 Disturbance and Variation Analysis in Manufacturing Systems course material, KTH, 2017
7. J.L. Hintze, "Taguchi Designs", [Online]. Available: https://ncss-wpengine.netdna-ssl.com/wp-content/uploads/2012/09/PASSUG1.pdf [Accessed: 18 - Aug - 2019], NCSS, Chapter 887, pp 887-1, 2008
8. A. Sfakianakis, C. Douligeris, L. Marinos, M. Lourenço, O. Raghimi, "ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends", ENISA, 2018
9. P. Katsumata, J. Hemenway, W. Gavins, "Cybersecurity Risk Management", IEEE, 2010

AUTHORS PROFILE

Erkan Yalcinkaya is an independent industrial Ph.D. candidate at Department of Production Engineering, Royal Institute of Technology, Stockholm, Sweden. Erkan is an experienced IT security specialist focused on access control technologies. His main research focus is security aspects of industrial manufacturing systems and production lines.

Daniel T. Semere is an Associate professor at the Production Engineering department of the Royal Institute of Technology, KTH. He received his PhD from KTH in 2005 and his Master of Science degree from the East China University of Science and technology in 1996. His research area includes variation and disturbance analysis in manufacturing systems and variation propagations in multistage processes. He leads and participates in several externally funded projects in the field. He has contributed to the research through several publications. He also gives lectures and run graduate and post graduate courses in multivariate process control, robust design, machine learning applications to fault detection and diagnosis in manufacturing processes.

Antonio Maffei was born in Benevento, Italy, in 1982. He received the B.E. and the M.E. degree in industrial engineering from the University of Pisa, Tuscany, Italy, in 2004 and 2007 respectively. Antonio received a Ph.D. degree in production engineering from KTH Royal Institute of Technology in Stockholm, Sweden, in 2012. He is currently an associate professor at the Department of Production Engineering in KTH Royal Institute of Technology in Stockholm. Dr. Maffei is Head of the research group named Digital Smart Production where he leads a number of KTH initiatives as well as European collaborative projects. Since 2008 he has been active in teaching activities at undergraduate and recently also at graduate level; consequently he has built up a strong pedagogical background. His current research interests include business models for advanced automation technology, assembly technology and engineering education. Dr. Maffei is a Research Affiliate of The International Academy for Production Engineering (CIRP) and the Swedish Production Academy, Sweden.

Prof. Mauro Onori obtained his PhD in 1996, has published over 150 articles in peer-reviewed conference proceedings, international journals and books, and is currently Head of Department of Productioin Engineering at the ITM School of KTH. He has written and obtained grants for over 14 European Commission projects (including as Coordinator for an Integrated Project, budget 40 M Euro), received the Japan Robot Association Award (1996), the Emerald Literati Awards (2001, 2014) and acted as consultant to companies and Scientific Advisor to Swedish and Norwegian funding organisations. Prof. Onori is an Editorial board member and Reviewer of the Assembly Automation Journal, Emerald Press.