NATIONAL UNIVERSITY
OF PUBLIC SERVICE
Doctoral Council

János Gerevich

Possible Applications of Agile Software Development Techniques for the Hungarian Defence Forces

Author's Summary of the PhD Dissertation

Budapest

2020

NATIONAL UNIVERSITY OF PUBLIC SERVICE
DOCTORAL SCHOOL OF MILITARY SCIENCES

János Gerevich

Possible Applications of Agile Software Development Techniques for the Hungarian Defence Forces

Author's Summary of the PhD Dissertation

Supervisor: Dr. habil. Imre Négyesi Lt. Col. PhD

Budapest

2020

DEFINITION OF THE SCIENTIFIC PROBLEM

The importance of IT systems for military purposes in the information society is continuously growing. These systems contribute to the enhancement of the armed forces and help support the sustainability of the defence capabilities. According to the Basic Law, the Hungarian Defence Forces is responsible for the protection of Hungary, to achieve this goal, high-quality stationery and temporary IT systems are required. The high-level support of the electronic administration and the uninterrupted external communication is essential in the proper organisation of the national defence. From this point of view, the Hungarian Defence Forces implement administrative processes which are similar to the governmental workflow - keeping in mind the hierarchical organisational structure and the daily operation based on the principle of military command.

The just mentioned administrative workflows and record management processes represent the bases of the official information flow between the defence sector bodies and external entities. Today, in majority of cases, different IT systems are supporting digital communication with other public administration bodies, legal entities and natural persons. The methods and technologies used to design information and communication systems in the defence sector have significant importance because the security and reliability indicators of the developed systems also have an impact on the overall security of our society.

Due to the spread of cloud-based solutions in the last two decades, the dissertation deals exclusively with software technology problems interpreted in a virtual environment - in cyberspace. The dissertation doesn't discuss physical metrics, network-, hardware- and environment-related issues comprehensively, only to the extent necessary to understand the given software development problem.

For computer science, I considered analysing the agile software development methodologies as the starting point of the dissertation, which were already used by 53%[1] of the companies engaged in software development worldwide at the beginning of my research. According to 2019 statistics this figure was already at 97%.[2] Recent surveys also show that a quarter of companies engaged in software development have been using the methods under study for more than five years. I believe that based on the statistics of the last four years, considering agile software development methodologies as a starting point was the right decision when starting the research. The specific problems examined in the dissertation are listed below:

[1] Based on data from an international survey on the state of agile software development in 2016.
[2] Based on data from a repeated study from the American website StateOfAgile.com in 2019.

• Can the Hungarian Defence Forces apply agile software development methodologies?
• What processes and document templates are required for the controlled execution of an agile software development project?
• What are the differences between civilian and military custom software?
• What design patterns and software architectures can arise during the application of an agile software development methodology for military purposes?

RESEARCH OBJECTIVES

The research aims to explore the above described scientific problem from software technology and defence perspectives. The further goal is to define software development methods and design patterns which can be used for ICT system developments for defence and general purpose. Within this, my primary research goal is to develop a hybrid agile methodology that can be applied to the project management and cooperation of a military organisation and a software company to achieve the best quality as a final result. The methodology includes the identification of appropriate roles and responsibilities in the design, development and testing stages. An exciting research opportunity is to determine the requirements for the necessary documentation for the phases of the project. What tables and templates are needed to perform each task? My goal is to develop unique techniques and methods that can be used to integrate special military requirements (vulnerability testing, fault tolerance, computing power loss, bandwidth reduction, switching between algorithms, etc.) into the software from the beginning. With this technique, a continuously developing military system can be created from the very first steps.

A further aim of the research is to identify and explore the architectural and software design patterns during the application of the developed methodology. In military IT systems where the hierarchical organisation is part of the model, IT professionals may face serious problems. The deletion or relocation of certain organisational elements can have an impact on the commands, deadlines, processes, responsibilities, roles and permissions issued so far. In these cases it is essential to calculate and model the successors so that continuity can be maintained within the given information system.

From the synthesis of modern technology and special requirements, new design patterns and solutions can be created, which can be used for an existing system upgrade or a new system development. After exploring and understanding the processes belonging to the applied agile methods, public procurement procedures and internal regulations for special software can be

prepared and developed. Based on these documents, the Hungarian Defence Forces can have adequate capabilities to announce and implement an agile software development tender.

RESEARCH HYPOTHESES

- Agile software development methodologies can be applied for military purposes taking into account the special requirements of different military disciplines.
- During a military application, the phases of an agile project can also be identified, for which appropriate documentation templates can be developed.
- Using an agile software development methodology more flexible and more realistic military software can be developed.
- New software design patterns can be identified during agile software development for military use, which can be widely applied in the future.

RESEARCH STRATEGY AND METHODS

By processing the foreign and domestic literature on agile software development and defence informatics and relying on my more than 15 years of personal software development and design experience, my goal is to develop a set of requirements to meet typical design, development and testing problems. During the research, I will use simplified examples derived from real issues for careful analysis of defence considerations and agile software development guidelines in mind. The selected samples are derived from electronic administration, military records management and other areas related to defence informatics, which I have had the chance to get to know comprehensively in my professional activities so far. Only unclassified and accessible literature is used in the research. I believe that the problem can be fully discussed on the basis of public information.

During my research, I will keep in mind both informatical expectations of defence and agile software development principles. At first, I will use a deductive method to develop the basic problem in the form of general and specific research requirements with accepted methods in software development, using generally known defence informatics, security and IT requirements. The set of requirements to be identified will be based on the publications and directives of the European Union, NATO project management standards, various security strategies of Hungary, as well as the current legislative environment related to the research and Hungarian Defence Forces' documents containing IT requirements. During the exploration of the literature examined by the research, the aim is to identify general IT,

project management, design, software development, service, operation, security and reliability (quality) requirements.

Based on the specified set of requirements, concerning the software technology and defence informatics a new software development methodology, the Military Scrum will be developed using inductive methods which meet the unique needs. The methodology is going to specify the process descriptions, documentation techniques and document templates, as well as software development procedures and operational recommendations required by the methodology.

Once the methodology has been defined, using examples linked to e-government and the processes of hierarchical organisations, the aim is to develop design patterns that meet the modern requirements and create services that operate safely, reliably and securely.

Compliance with the research requirements identified during the deductive phase takes two steps. The specific research requirements are mostly satisfied with a software development methodology that enables military applications and software design models that support the operation of military organisations. With the help of these two exact results, the verification of the research hypotheses could be realised. The satisfaction of the general requirements revealed during the research can be attained by using the exact results – in addition to the verification of the research hypotheses – by presenting the possible applications of the research results.

SUMMARY OF THE CHAPTER 1

During the exploratory work of Chapter 1, the regulatory framework related to the protection of critical infrastructure protection in the European Union and Hungary was reviewed. As a result of the analysis, the general identification, designation, review and registration processes were also discussed. Finally, the defence sector-critical infrastructure protection for the Hungarian Defence Forces was also shortly reviewed finding a link between critical infrastructure and the operation of the defense sector.

Subsequently, specific regulations for essential IT systems were discussed from the perspective of network and information security, resulting in the identification of eight general information security research criteria in addition to a comprehensive discussion of cloud computing service models.

In the final section of the chapter, further specific and general research requirements were identified by examining the cybersecurity aspects of various security strategies of Hungary.

SUMMARY OF CHAPTER 2

In Chapter 2 of the dissertation, the current IT documents of the Hungarian Defence Forces were reviewed from a software technology perspective. In parallel with the analytical work, the strategic objectives of the armed forces for ITC were also examined.

During the analysis, four general methodological requirements were identified based on the IT Regulations of the Hungarian Defence Forces. After that, twelve special IT requirements analysis have been carried out, which are coming from the Joint Doctrine of Informatics and can be interpreted from software technological aspects. Finally, after a comprehensive examination of the regulatory documents, it became possible to formulate five specific criteria about requirement analysis methods.

SUMMARY OF CHAPTER 3

Concluding the deductive phase of the research, NATO's military capability development methodology SLCM covers the entire life cycle of military system development and provides the appropriate model and processes for this. During the analysis we were able to see the life cycle divided into stages, as well as the scope and activities of each stage. In line with the research objectives, methodological, technological and documentation requirements that could be interpreted from the software technology aspect were identified.

During the analysis of the NATO SLCM Directive, seven software technology requirements and three methodological requirements were identified. In NATO AAP-20, which presents the life cycle model, twelve methodological and three documentation requirements for software development have been defined. Finally, based on the analysed processes two methodological requirements for compliance with an essential AQAP standard have been identified. Later two software technology and seven documentation requirements were worked out.

SUMMARY OF CHAPTER 4

In Chapter 4, we learned about the possibilities offered by current software technology and reviewed the basics of agile software development and Scrum software development methodology. Subsequently, Scrum was placed in the project management triangle. Then we saw that the occupied place by the method was suitable for governmental application, as well as within the defense sector.

Then, the Military Scrum software development methodology was defined with a systematic definition process, taking into account NATO SLCM processes and Scrum methodology.

During the process, it was assumed that the primary scope of the developed methods is the development and support of software-based services. The work was supported by the requirement analysis (R) criteria identified in Chapter 2. Later the life cycle stages, roles, tasks and documentation templates used by Military Scrum were determined - to support the following activities:

1) Requests – Pre-concept;
2) Creating the set of requirements – Pre-concept;
3) Defining the requirements – Concept;
4) Preparation of acceptance tests for handover process – Development;
5) Recording the error tickets – Support;
6) Change on-demand request – Utilisation.

Agile software development techniques have been identified to support the development phase that guarantees the complianceof the installation kits required for the utilisation of software-based services from both methodological and technological point of view: TDD, DDD, CI, etc. Later, there were identified process-level requirements for the environment, as well as the concept of an integrated operational platform (IOP), which together make it possible to achieve the appropriate level of operation performance after the stage of development. Compliance with security requirements and monitoring infrastructure were also taken into account when methods were defined.

SUMMARY OF CHAPTER 5

Chapter 5 also presents the scope of the GDPR [7] and the definitions of concepts that can be related to general data operation activities: data subject, personal data, data processing, processor and controller. We have learned that Member States have been exempted from implementing the GDPR in the defense sector, on the assumption that in this sector at least the regulations or stricter rules are prevalent. After this, personal data of the data subjects and the related data management activities from the perspective of CRUD operations were examined, which also highlighted the deficiencies of the primitive model in terms of data modification and physical deletion. The explored weaknesses were fixed by the combination of the attributes of the Proxy and Holder design patterns. The SubjectHolder design pattern was defined, which shows appropriate behaviour for CRUD operations performed on the affected data subjects - also for parallel data operation activities.

The concept of the data subject in GDPR terminology covers natural persons. Besides, the *SubjectHolder* design pattern can be extended to model hierarchical organisations using the *ResponsibleHolder* and *PartyHolder* design patterns derived from *SubjectHolder*. The operation of design patterns has been determined with the help of case studies from the administration. Still, their use can be an alternative for any military application to model the hierarchy and implement application-specific processes. Then, in addition to presenting the administrative processes of the Hungarian Defence Forces – by interpreting the relevant legal requirements – additional design templates were developed to support electronic administration processes in the form of the *Package*, *IncomingPackage* and *OutgoingPackage* design patterns. In the closing part of the chapter, the possible applications of the specified design patterns were presented to support the legal level defined processes of the electronic records management systems – thus providing an insight into special application possibilities of the design patterns identified during the dissertation.

SUMMARY CONCLUSIONS

At the beginning of my research, I set up four hypotheses, for the verification of which I first analysed the regulatory framework of the European Union and Hungary concerning cybersecurity from a software technology aspect. Then I explored the development and operation of software-based services in the light of NATO's military capability development methodology and the IT requirements of the Hungarian Defence Forces. During the exploratory work, I identified and systematised eighty-four different research criteria. I classified the specified conditions into cybersecurity, methodology, software technology, information security, quality assurance and documentation categories, as well into special and general levels.

The specified set of requirements allowed me to start the inductive phase of my research with sixty special expectations. The primary goal of which was to synthesise agile software development techniques and standard military capability development methods. To confirm my first two hypotheses, I considered defining an appropriate military software development methodology that combines NATO SLCM processes and Scrum [8] agile software development methodology as a hybrid solution. The described methods satisfy the specific requirements; the significant differences between the analysed and defined techniques are shown in Table 1.

	Scrum	NATO SLCM	Military Scrum
Roles	ScrumMaster, Product owner, Development team	Not defined exactly, it is based on the ISO 15288 standard organisational process	Customer, Project Manager, ScrumMaster, Product owner, Development team, Operations
Scope	Software development	General military capability	Development of software-based services
Stages/steps	Sprint planning, development	Preconcept, Concept, Development, Production, Utilisation, Support, Retirement	Preconcept, Concept, Development, Deployment, Utilisation, Support
Iteration handling	one level: development sprints	one level: modification and upgrade procedure	two levels: Military Scrum development rounds; sprints in the development stage
Documentation	Product backlog (Story) Sprint backlog (Task) other documents of development and testing	D-1, D-2, D-3 specal research criteria contain the interpretable documents from a software development perspective	Requests, Set of requirements, Requirements, Sprint backlog, Handover test scenarios, Bug list, Change requests

Table 1 Comparison of Scrum, NATO SLCM and Military Scrum methods (by the editor)

The Military Scrum software development methodology specification has been implemented successfully; the number of the required documentation has been reduced in favour of modern technologies, so that the capabilities of the methodology are still suitable for military application based on NATO requirements. Compliance with each requirement is described in Annex 2 of the dissertation, also, compliance with the documentation requirements required by the SLCM when applying Military Scrum. Thus, the developed methodology is also an alternative for the Hungarian Defence Forces for the development of software-based services for military purposes.

To verify the remaining two hypotheses, I examined the administrative processes performed by the Hungarian Defence Forces and the issue of electronic administration from the perspective of the implementation of primary data (CRUD[3]) operations. I interpreted the performance of operations on the organisational elements that make up the hierarchical structure, assuming their parallel data management activities with the GDPR principles in mind: purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.

As a result of the research, I developed general design patterns that support parallel, GDPR-compliant data management processes for hierarchically structured organisations so that they can be used in different military applications.

[3] CRUD – the acronym based on the starting characters of the primary data operations: **C**reate, **R**ead, **U**pdate, **D**elete

EXAMINATION OF RESEARCH HYPOTHESES

I identified fifty-eight special research criteria with the exploratory analysis of the NATO SLCM processes, the relevant documents of the Hungarian Defence Forces in IT scope, and the components of the Hungarian and EU cyber defence strategy. This analysis allowed examining research hypotheses 1 and 2. The identified research criteria based on the current legislation of the Ministry of Defence and the Hungarian Defence Forces, the GDPR directive on data protection and the NIS directive allowed the discussion of hypotheses 3 and 4. The specific information security requirements (I-9) and (I-10) in Annex 2 can be met by the combined use of the Military Scrum and Holder based design patterns.

Hypothesis 1: Agile software development methodologies can be applied for military purposes taking into account the special requirements of different military disciplines.
The Military Scrum software development methodology identified during the inductive phase of the research uses agile methods and techniques to support the development of software and software-based services. The specified methodology meets the identified NATO and Hungarian Defence Forces requirements; therefore, it can be used for military purposes. The answers to the special research requirements given by the methodology can be found in Annex 2 of the dissertation.
Based on the research results, I consider Hypothesis 1 to be justified.

Hypothesis 2: During a military application, the phases of an agile project can also be identified, for which appropriate documentation templates can be developed.
Military Scrum defines a six-stage iteration for the entire software development life cycle: pre-concept, concept, development, deployment, utilisation, support. The methodology provides a project management template to support software development project processes. It assigns the appropriate tables to each stage: requests, requirement sets, product backlog, sprint backlog, acceptance test scenario, bug list, change requests.
Based on the research results, I consider Hypothesis 2 to be justified.

Hypothesis 3: Using an agile software development methodology more flexible and more realistic military software can be developed.
Based on the administrative processes of hierarchical military organisations, by examining CRUD operations performed in parallel on the data of natural persons and organisational

elements, flexible and realistic design patterns were developed. The developed design patterns support the function of physical deletion and the separate handling of historical and maintained data. They can be applied both to the data of natural persons and to other entities that are part of the military hierarchy - the possibility of military use is supported by the methodological and technological requirements prescribed by the Military Scrum.
Based on the research results, I consider Hypothesis 3 to be justified.

Hypothesis 4: New software design patterns can be identified during agile software development for military use, which can be widely used in the future.
The identification of *SubjectHolder*, *PartyHolder*, *ResponsibleHolder* and *Package* design patterns was accomplished by analysing CRUD operations performed on natural persons and organisational elements in the light of use cases. The procedure is analogous to the TDD and DDD methods prescribed in the Military Scrum software development methodology. The descriptions of CRUD operations are the test scenarios, and the specified design patterns are representing the established business domain. The specified design patterns are universal, with an appropriate software technology background they can be used by the government and the private sector to implement administrative and communication processes.
Based on the research results, I consider Hypothesis 4 to be justified.

NEW SCIENTIFIC RESULTS

- I was the first to develop twenty-four criteria that take into account the requirements of defence developments, promote general cybersecurity and focus on practical usability.
- I created a special NATO SLCM compliant set of requirements to complement software development methodologies for military use.
- I specified the Military Scrum software development methodology, which meets the special requirements of the research.
- I placed the parallel data management processes in hierarchical organisations workflow in a model under the GDPR principles, and based on this, I developed research criteria based on military administrative workflows.
- I have defined *PartyHolder*, *ResponsibleHolder* and *Package* design patterns that support parallel data management processes and can be applied to organisations operating in a hierarchical structure.

PRACTICAL APPLICABILITY

The twenty-four general research requirements explored in the first half of the dissertation have at least as many practical applications. The following are the general requirements identified from different research areas and the practical applications of the scientific results of the research.

1) The security shall strive in the development of information systems linked to different security complexes, in particular military security. The Military Scrum software development methodology elaborated during the verification of research hypotheses enables the development of software-based services that have consistent security and reliability indicators throughout their lifetime. The methodology can be applied to the development of information systems in the military security complex, as it was created by interpreting the development processes of software-based services in the NATO SLCM. Security requirements can be integrated into the criteria of projects implemented with the methodology from the pre-concept stage. Military Scrum supports development and operation with procedures that guarantee the implementation of security requirements and their subsequent maintenance throughout the entire lifetime of systems. The application of techniques is not only possible within the military security complex. They can also be applied by economic and governmental actors during the implementation of their software development projects.

2) The development of ICT procedures and methods that ensure adequate defence and response capabilities is required. In this area Military Scrum provides technology and practices for the design, development, operations, utilisation and support of the unique software-based services, including the interpretation of security requirements. The software developed by the methodology can be built with protection and response capabilities from the early start, thanks to the integrated management of security requirements.

3) Computer networks and related information systems must be prepared for coordinated attacks. For software-based services at the top of the cloud-based service model, Military Scrum can be used to build automated system management capabilities in the SaaS layer as part of security requirement analysis, development, deployment and support. If incidents of the same nature are encountered within different information systems by the automated

system management, it can be assumed that this is a coordinated attack and that uniform cybersecurity protocols can be applied.

4) The development of ICT systems has to ensure close cooperation and efficient information exchange for the actors of the defence sector. The Responsible Holder and Package software design patterns can support the administrative processes and the communication within hierarchically structured organisations and external information exchange that meets the requirements of the GDPR. The software development processes specified during the research and the design patterns based on their application will present an alternative for the future development and integration of the ICT systems in the defence sector.

5) IT systems must have monitoring tools that allow them to support perception, processing and detection activities. Military Scrum already provides the capability for prototypes produced in the first development phase to meet the requirements for detection, processing and reaction activities. After that, it is possible to maintain and increase capabilities in the integrated implementation, support and utilisation phases. Continuous change handling of the operation environment is a criterion for the development, which allows the software-based services to share information with the integrated operations management software about unusual activities. With this technique, the technical reports of the services can be extracted and processed. The detection of external and internal causes and factors can be done based on the processed information.

6) Risk management should be supported through appropriate methods, both within and across sectors. The Military Scrum requirement refining technique on the sets of security criteria could support a comprehensive risk analysis of cybersecurity threats across all sectors. When the method is applied, risk management expectations for all sectors emerge by the end of the risk analysis process - the resulting document is a security product backlog. This document can serve as a starting point for the implementation of sector-specific risk management procedures, the refinement of which can also lead to the identification and management of sector-specific risks through the execution of the method. By processing the results together, an integrated cross-sectoral risk management concept can be created.

7) It is necessary to provide an appropriate set of tools for risk analysis and risk management to develop and support appropriate response procedures to cyber threats. If the response to the cyber threats is implemented by IT systems - software-based services, not only the risk analysis can be supported, the Military Scrum software development methodology can also be used for the implementation of the risk management systems. In this case, the methodology presents the toolset that can be applied from the risk analysis until the operational response procedures.

8) The new methods must support the quick detection, assessment and risk analysis. In the case of intentionally launched cyberattacks against software-based services, if the goal is not to make the infrastructure down, the standalone defence capability of the given IT system becomes essential. Military Scrum enables the quick detection and signalling of cyberattacks in the case of operating infrastructure, by interpreting the set of security requirements, defining special security functions and then including them into the developed software. If the way to deal with the detected incidents is already available, they can be performed automatically within the system. The methodology allows the inclusion of experience into the safety requirements in subsequent risk analysis.

9) One should strive for reliability during design and development. During the pre-concept stage of software development projects implemented with the Military Scrum methodology, the critical reliability requirements can be included in different sets of criteria by the customer and the product owner. Further stages of the methodology will ensure their implementation. It is also essential that in the third step of the requirements analysis techniques provided by the methodology, during the sprint planning, the product backlog elements of the system are analysed and split into feasible tasks. During the process, an expert (product owner) who is aware of the meaning of the requirement - even the history of its origin - talks to a development team with the appropriate expertise. Hence, the first step in the design induces functional reliability.

10) In the cloud-based operations environment the services must be developed with sufficient reliability and security parameters. The cloud-based operations environment assumes that a third party performs the infrastructural operation of the software-based service. There is a need for a development methodology where the capabilities of the developed software can be separated from the operations environment. It allows managing the reliability

and security parameters of the operations environment and the developed software separately. The Military Scrum software development methodology separates the development and deployment phases, allowing verification of the reliability and security requirements for the developed software before the deployment. If the deployment involves installation in a cloud service, the prerequisite check and testing can then be performed for the safety and reliability of the operations environment.

11) The goal to be achieved is applying high-level security and reliability standards. From the software technology side, Military Scrum provides tools for a high level of security and reliability for software and software-based services. The methodology might represent the basis for the innovation of new software technological standards.

12) Detection of security incidents, revealing and the correction of logical errors has to be done by standard procedures and methods. Using Military Scrum, you can develop automated system management solutions that can detect known, relevant security incidents for a software-based service, either in-house or in a third-party operations environment. Monitoring the errors in the operations environment of the service can also be implemented with the technique. Based on the gathered information, in the next development stages, there is an ability to correct verified logical errors and handle identified security incidents. Those can be implemented with controlled procedures within the developed software.

13) Regulated methods and processes must support the creation of security plans. In the development processes of Military Scrum, the security criteria and the development tasks about security that can be derived from them can be handled separately in the first two phases.
risk analysis → definition of the security set of requirements
risk management → definition of security requirements and responses (can also be part of the product backlog)
toolset → automated testing, application specific tools (development of incident management capabilities for the developed software)

14) The security incidents have to be manageable, detectable and reportable with appropriate information. If the Military Scrum software development methodology and the requirements of operations environments were widely used as a standard, the following reporting model could be introduced. It is possible to define an appropriate conventional

incident code for each incident type, similar to HTTP error codes, which would allow the central incident collection for essential systems. This technique could allow us to manage and report cyberattacks on essential software-based services globally.

15) Design methods that can guarantee the reliability of the essential services and handle security aspects are required. In the development process of Military Scrum, it is possible to review security aspects and supplement them based on cybersecurity experiences. If another threat emerges in cyberspace, it can be handled at the software level and analysed in the conceptual stages. If response procedures can be integrated into the developed software against the emerging threats, their development can be implemented within the development stage, thus guaranteeing the continuous operability in the light of the known risks.

16) The correspondent reaction capability can be fostered by specialised system management solutions that immediately can detect the changes in essential services and alert potential security incidents. The supervision of the digital infrastructure and the protection against various cyberattacks are managed at the level of the European Union and the government. If any software developed by Military Scrum methodology were to be identified as an essential service, the integrated management of requirements for the operations environment and the developed software would be given. The methodology allows creating reliable, responsive capabilities because of evolutionary software development techniques. Incidents detected by the software can be channelled into the operations system control so that software level incidents can also be visible in addition to infrastructure and network security events.

17) It is essential to have a quick changeability throughout the life cycle of IT systems. With the help of the appropriate level of support, for a change request can be quickly decided if the current system concept or its extension or modification is required for the implementation. The latter case is rare for already deployed software-based services. With the appropriate application of Military Scrum and the evolutionary software development technique, the effects of requirement changes can be analysed in the automated test execution infrastructure within a short time. After that, the only task is to restore the consistency of the system in light of the new requirements. The changes are released when the next software installation package is prepared and can be deployed via automated deployment procedures defined by Military Scrum.

18) During the development of new systems, it is necessary to establish sustainable, continuously updatable technical bases. The appropriate application of Military Scrum to the developed software means that the behaviour of the system is also documented in the form of automated tests. This approach allows to upgrade a component of a software-based service, if needed and the maintenance can be performed with little risks. The evolutionary software development technique enables the consistency check and system verification for a new component. The deployment process defined by the methodology provides feedback about new parts behaviour before utilisation, but already in the operations environment.

19) In the case of newly developed IT systems, continuous inspection of security requirements should be part of the development process. The technique of evolutionary software development does not make a difference between technical, functional, and security requirements. If the Military Scrum sets of requirements adequately reflect the security criteria for the developed software, their evaluation will be continuous throughout the entire life cycle in the development phases.

20) In the case of essential systems verification of security requirements and vulnerability testing sector should be an independent part of system developments. Of course, legal regulations are also needed to implement this requirement. However, Military Scrum provides an opportunity to integrate automated vulnerability testing in the evolutionary software development environment of the software. In the deployment stage during the handover phase after the installation on the migration environment, repeated tests can also be performed in the operations environment to ensure correct configuration and behaviour for vulnerabilities. Thus, software-based services developed with the methodology can have double protection.

21) IT services should be changeable with minimal resources and time and adaptable for changing user needs and application circumstances. Fulfilment of the methodological requirement is possible when the maturity level of the enabling systems for the given software-based service reaches the appropriate level - according to the NATO SLCM System Concept. The adequately applied Military Scrum ensures efficient work, fast implementation velocity meeting the user's requirements. Preparing for changes in the operations environment can be achieved quickly and efficiently during the development and deployment phases of the methodology.

22) The development and provision of ICT services should be implemented based on the operational requirements of the applying organisations, the professional needs of the organisations responsible for ICT, the technical specifications of the procurement, the system plan of the service to be developed, the application plan of the user organisation and the legislation and documents regulating the activity. The Military Scrum requirement analysis methods allow the collection of listed needs assigning them to the responsible entities. Further, in the first two steps of the requirements analysis process, the demands from the different levels of the organisation can be included into the system criteria. Based on this the concrete requirement sets and the product backlog can be specified. The iterative refinement process can be used to resolve anomalies in the system criteria. During the pre-handover development sprints, the functional requirement system, the developed software documentation and the application plan can be refined.

23) The aim is to develop a software development methodology that supports the provision, planning, development and supervision of ICT services and can be interpreted for the entire life cycle of the systems. The Military Scrum methodology is based on NATO SLCM and meets this research criterion.

24) It is necessary to develop a methodology that supports the analysis of suggested developments and the identification of change request in a regulated manner. The Military Scrum methodology requires the analysis of change request during each development round, both in the pre-concept and concept stages. The process takes place in a regulated way in the 1st development round, in the pre-handover period and also in the case of an utilised system.

RECOMMENDATIONS

1. I recommend the application of the Military Scrum software development methodology in the documents and processes regulating IT developments in the Hungarian defence sector, thus creating transparency and interoperability between customer and supplier processes.
2. I propose to introduce the development and operation standards defined by the Military Scrum into the software development and operation processes for essential services.

3. For further research, I recommend the possibilities of integrating measurement procedures of unique software technology (S) requirements (efficiency, flexibility, deployability, etc.) into the evolutionary software development environment used by Military Scrum.
4. I recommend the use of *PartyHolder*, *ResponsibleHolder* and *Package* design patterns in every IT system that model hierarchical organisational structures and implement data management processes performed in parallel, including government and enterprise use.
5. I urge professionals involved in the development of electronic records management software to use the design patterns defined in the dissertation when modelling the domain specified in the legal obligations.

PUBLICATION LIST OF THE CANDIDATE RELEVANT TO THE DISSERTATION'S TOPIC

[1] GEREVICH J.: Az agilis szoftverfejlesztés alkalmazásának lehetőségei a Magyar Honvédség számára. In: Hadmérnök XII. 1. (2017) 170-181. o.

[2] GEREVICH J.: Híradó-Informatikai fejlesztést támogató agilis dokumentációs módszerek. In: Hadmérnök XII. 3. (2017) 210-222. o.

[3] GEREVICH J., NÉGYESI I.: Híradó-Informatikai fejlesztést támogató agilis dokumentációs módszerek - 2. rész. In: Hadmérnök XIII. 1. (2018) 230-244. o.

[4] GEREVICH J., NÉGYESI I.: A Military Scrum követelményelemző módszerének alkalmazása létfontosságú rendszerek fejlesztése során. In: Hadtudományi Szemle XI. 3. (2018) 293-304. o.

[5] GEREVICH J., NÉGYESI I.: A Military Scrum szoftverfejlesztési módszertan alkalmazása létfontosságú infokommunikációs rendszerek fejlesztése során. In: Hadtudományi Szemle XI. 4. (2018) 72-82. o.

[6] GEREVICH J., NÉGYESI I.: A fenntartható és zavartalan elektronikus ügyintézés szoftvertechnológiai háttere - 1. rész In: Hadmérnök XIV. 2. (2019) 281-292. o.

[7] GEREVICH J.: Software Technological Interpretation of the NATO Military Capability Improvement Process. In: AMERICAN JOURNAL OF RESEARCH EDUCATION AND DEVELOPMENT IV. Évfolyam 3. szám (2019) 28-35. o.

[8] GEREVICH J., NÉGYESI I.: A fenntartható és zavartalan elektronikus ügyintézés szoftvertechnológiai háttere - 2. rész In: Hadmérnök XIV. 4. (2019) 75-89. o.

[9] GEREVICH J., NÉGYESI I.: Network and Information Security of Cloud Computing Services. In: Hadtudományi Szemle XIII. 1. (2020)

SCIENTIFIC-PROFESSIONAL BIOGRAPHY OF THE CANDIDATE

Name: János Gerevich

Date of birth: 07. 05. 1984.

E-mail: gerevich.janos@agilexpert.hu

Workplaces

Year	Position	Workplace
2013–	Managing director	AgileXpert Software Development Ltd.
2016 2015	IT consultant Lead software developer	HM EI Co. IT Directorate
2012–2013 2010–2011 2009–2010	Development manager Lead software developer Sofware developer	Synergon System Integrator Ltd.
2008–2009 2007	Junior software developer Intern	Synergon Informatika Nyrt.

University studies

Year	Research field / university degree	Institution
2016–	Theory of defence informatics and communication (PhD)	NKE HDI
2002–2008	Computer science (MSc)	ELTE TTK, IK

Scientific and educational activities

Year	Activitiy	Institution / Location
2018	Presentation: High-level IT services in the cyberspace	Communication 2018 Scientific Conference
2017	Presentation: Agile software development methods and their use in robot techniques	Robot Warfare 2017 Scientific Conference
2016–	11 publications, link on MTMT's surface: https://m2.mtmt.hu/gui2/?type=authors&mode=browse&sel=10073524	NKE HDI
2014–2015	Teaching programming subjects as a commissioned external lecturer.	NKE HHK Department of Informatics

Foreign languages

English: intermediate (C), BME Language Examination Center (2016)

Ukrainian: advanced (C), Foreign graduation certificate (2002)