Risk Management in Development of Croatian Maritime Cargo Single Window System

S. Aksentijević[*], E. Tijan[**], K. Nikolozo[***] and A. Perić Hadžić[**]
* Aksentijević Forensics and Consulting, Ltd., Viškovo, Croatia
sasa.aksentijevic@uniri.hr
** University of Rijeka, Faculty of Maritime Studies/Department of Maritime Logistics and Management, Rijeka, Croatia
edvard.tijan@uniri.hr, ana.peric@uniri.hr
*** Bartolići 6, Zagreb, Croatia
kristijan.nikolozo@gmail.com

***Abstract* - The aim of this paper is to research and describe the effectiveness of the risk management approach used during implementation of the Croatian national maritime Single Window system related to cargo, or Port Community System, initially in the port of Rijeka. The primary stakeholders and their internal systems, as well as formal development requirements, are defined. Project risk is identified within the project management framework's criteria, and the project's execution and important milestones, including risk occurrences during project execution, are recognized and discussed. Finally, modifications to the approach are suggested, as well as future study opportunities.**

Keywords – Single Window System, Port Community System, Port of Rijeka, risk management

I. INTRODUCTION

The major purpose of the Croatian maritime cargo Single Window system (or Port Community System - PCS) implementation project in the Port of Rijeka is to connect all port stakeholders, including government and commercial entities and their digital information systems to the Croatian Integrated Maritime Information System through a single digital platform (CIMIS) [1] [2]. The construction of the Croatian Port Community System began in late 2017, when the Port of Rijeka Authority received funding from the INEA [3], in the form of the Connecting European Facility – POR2CORE – Port Community System project [4]. The project was overseen by the Croatian Ministry of the Sea, Transport, and Infrastructure [5] and managed by the Port of Rijeka Authority. The main goal of the project was to align the implementation activities with other ongoing digital technology developments in the maritime sector, and to create a system that could be used in other Croatian cargo ports after the initial pilot project in Rijeka is successfully completed.

With the project's ambitious scale, numerous interested parties, limited finance, and rigorous contracting conditions and deadlines, it was clear from the start that there would be several major groups of risk sources. For this reason, work began on identifying a risk framework that would be appropriate for tracking the evolution of such a complex system with numerous internal and external stakeholders and risk types. After internal analysis, it was decided to adopt traditional enterprise risk management approach and monitor its performance and capabilities. This approach was used over the course of the project's four years of execution.

The risk management procedures during time and money constrained complicated cargo marine Single Window projects are scarcely and incidentally studied and have not been well addressed. The majority of prior research has focused on general and top-level risk management. The tracking of project risks is frequently entrusted to senior management, who are responsible for monitoring project risks and mitigation activities, which must be consistent with expected timetables [6]. Based on prior experience, some authors argue that the costs of implementation may be larger than the benefits in some circumstances, rendering whole implementation initiatives worthless from a pure financial standpoint [7]. The majority of risk assessments for maritime cargo Single Windows are centred on their economic feasibility. Some writers acknowledge that there is a lack of maritime cybersecurity awareness, as well as the significance of a comprehensive strategy based on hazards and maritime cyber risk valuations linked with maritime authorities and identification of critical assets in this sector [8]. Researchers that are more technically oriented in their studies adopt a different approach, and their perspective of hazards during project execution is restricted to features of the underlying technology, digital components, and cybersecurity. They acknowledge that, until recently, ports were primarily concerned with physical security. However, cyber assaults pose the greatest threat today [9], so there is pronounced need for approach change.

As a result of previous research, it appears that during the development of complex cargo maritime Single Window systems, there is a disjointed approach to risk analysis and management methodology, where different stakeholders, based on their previous experience with separate segments of the system, take a different approach to individual risk types and mitigation measures, rather than an integral model approach. Quantitative advantages may be assessed using traditional project management methodologies as well as financial indicators and approaches, but qualitative benefits are best realized through strategic analysis.

II. PCS Development Requirements

Interoperability with existing IT systems of individual stakeholders of the port community, the CIMIS NMSW system, and the Republic of Croatia's eCustoms system, was the primary requirement that PCS had to accomplish in order to achieve the project's intention [10]. It was created with the following implementation goal in mind: to enhance and ease the optimal flow of information between participants in integrated maritime and land transportation systems employing integrated components. The most important needs are the simplicity and optimization of business operations among port community members, single data entry, and data confidentiality, integrity, and availability. It had to be adjusted to the port of Rijeka's design and operative construction, which has four distinctive, independent port basins [11].

Port Authority, Harbor Master's Office, Ministry of the Sea, Transport and Infrastructure, Ministry of the Interior (border police), Customs authorities, maritime carriers, port concessionaires - terminal operators, maritime agencies, shipping companies and transport organizers, land carriers (rail and road), sanitary inspection, phytosanitary inspection, veterinary inspection, and other administrative services are among the most important stakeholders in the Rijeka PCS development project. Therefore, it had to be designed to accommodate their needs, but also additional stakeholders in the port community. Stakeholders in the PCS system are involved in goods transportation and associated operations, although their scope varies, and it is dependent on each company's profile and activity. Each future stakeholder must be able to secure its own data, with the ability to manage the data for which they have been granted permission and approved access.

Figure 1 shows the orchestration of various stakeholders via interconnected systems and PCS modules.

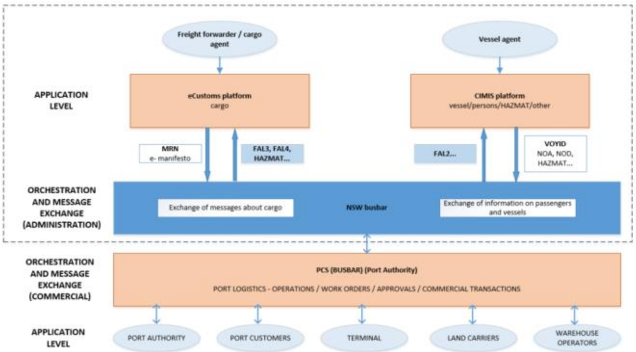

Figure 1: PCS connections orchestration

Identified PCS modules use the following codification:

1. D1 - official procedures of maritime administration and exchange of the information with the NMSW CIMIS system;
2. D2- ECS (Export Control System) and ICS (Import Control System) modules – exchange within customs procedures prescribed by the Ministry of Finance;
3. D3 - port container terminals operations;
4. D4 - NCTS (New Computerized Transit System) module – exchange of transit customs procedures data;
5. D5 - customs module – exchange with the eCustoms system, local risk control and integration with user applications;
6. D6 - port coordination and task planning;
7. D7 - access to the port area - control of vehicles and persons in the port area under ISPS rules and connection with truck announcement system (PORTUNUS);
8. D8 - conventional cargo warehouse operations – exchange with conventional cargo warehousing systems, delivery and dispatch of goods by sea and land, handling of containers;
9. D9 - hinterland container terminal operations;
10. D10 - CFS (Container Freight Station) module - container manipulation orders at the container terminal, storage and warehousing and
11. D11 - AGCT (container terminal operator) Rail module for rail container traffic - railway wagon operations.

Therefore, PCS has to be connected to the following varied information systems utilized by port operations stakeholders in order for all these modules to be effectively constructed and placed into operation: CIMIS, eCustoms, TOS F4B, TOS COMBIS, TOS NAVIS, TOS AGCT CFS and PORTUNUS. These systems are developed by the Ministry of the Sea, Transport and Infrastructure, Croatian Customs office, and cargo concessionaires to facilitate various aspects of the cargo operations in the port.

III. Project Execution

It is worth noting that, according to the original contract annexes, project plans do not foresee critical path milestones; instead, project execution was atomized in order to maximize available financial resources and deploy as many modules and capabilities as feasible, departing from the original plan. However, this appears to be a logical result of differing levels of participation in the project by diverse parties, particularly concessionaires. According to the initial project plan, critical milestones were (1) the creation of module D1 in the supplier's environment, (2) the installation of hardware and network components, and (3) the development of the overall functional specification. The first and second milestones were met; the third milestone was not, but they proved ultimately not to be important for the overall project's success.

Each step of the project execution was defined by the occurrence of a number of risks, which resulted in annexes to the original contract, scope extensions, and the dynamics of project development. The first significant milestone after formally commencing project development and integration in May 2019 was the preparation of a functional specification for the complete PCS system and development of the CIMIS interconnection module in the supplier's test environment. Due to challenges with the initial project kick-off and supplier team organization and cohesion, minor delays in hardware and integration services delivery, shifts in the focus of different stakeholders (concessionaires, customs), and the fact that the national CIMIS system was not ready for bidirectional communication, it was clear that a change in the project plan would be required. As a result, the service provider was unable to provide a complete functional specification for the system. The first appendix [12] to the original contract was stipulated in May 2020, formalizing the necessary adjustments. Functional requirements for individual modules shall be given simultaneously with module acceptances, according to this annex. The hardware was delivered and installed at the actual locations in the summer of 2020.

There was still no bidirectional connectivity with the national CIMIS system by the middle of 2020, which was a requirement for future integration. While some concessionaires have begun internal studies to assure conformity with the PCS, others have not. For the integrated modules, the provider has begun offering maintenance and helpdesk services. There was an open opportunity to extend the project for one more year, so late in 2020, a second annex [13] to the original contract was stipulated, and the financial value was increased by 17% due to the operational costs of the system (licensing, data links, and other costs) for one more year of development, as well as the need to develop three additional software modules, The year 2021 saw significant developments, and various modules were completed during that time, including the access control module (D7). After the Ministry's development services provider delivered the new version of the national CIMIS system to production in mid-2021, with bidirectional communication capabilities, related module D1 was completed. Customs-related modules (NCTS, ECS/ICS), as well as the planning and control portion of the D6 module for Luka Rijeka j.s.c concessionaire, were also released into production exploitation.

Further delays have been caused by the late development of interconnected systems by other parties, as well as the lack of concessionaires' availability for testing and development. To address this situation, the third annex [14] to the original contract was stipulated at the end of 2021, and with the approval of the INEA agency, the project execution was extended for one more year, until the end of 2022, and itemized prices were negotiated with the supplier in order to ensure development services coverage during that period.

The PCS system was placed into production in January 2022, with Port Control Center (LKC) [15] being the first user of the system in production mode and plans to immediately roll out modules D6 and D7 for concessionaire Luka Rijeka j.s.c.'s planning and coordination. Furthermore, project technical assistance team has created a set of public procurement documents for future maintenance services that was published on the Republic of Croatia's public procurement web early in 2022 [16]. This marks the official commencement of the national PCS's production operation.

IV. Project Risk Management

As a part of bidding documentation, only a few risks were anticipated, thus it was suggested that the supplier provides and explains the model for managing any negative project impacts that it expects to encounter during the project's execution, and that the client's acceptance be considered. By managing potential adverse effects during project implementation, the supplier should have ensured timely detection and effective management of potentially critical external or internal impacts and events, as well as propose effective preventive methodology to eliminate, transfer, or reduce the level of impact of adverse effects on the PCS development project. The technique of communicating with the customer, harmonization of diagnostics, degrees of risk, and harmonization when planning the treatment of undesirable effects are all part of the process of controlling probable adverse effects on particular project components.

Initial potential negative impact identification, as well as the likelihood of occurrence, impact on the project, and strategies to remove, transfer, or decrease the degree and severity of the negative impact have been identified. The risks were classified into four categories: 1) strategic, 2) operational, 3) technical, and 4) regulatory risks. This internal risk registry was eventually utilized as a source of data for the ongoing risk management.

The purpose of mapping identified risks was to make a connection between the PCS implementation project's risk management approach and enterprise risk management goals by emphasizing positive occurrences while avoiding or controlling negative ones [17]. Initial risk management matrix employed a proprietary enterprise project management risk registry. All risks identified and controlled during the project execution until the production work of the first module are processed using the same framework.

Initially, the project risk management strategy was based on standard enterprise risk management methodology as defined by the PMBoK (Project

Management Body of Knowledge) [18], with the goal of identifying not just hazards but also opportunities during project execution. Traditional project management approaches group risk sources according to different criteria with a focus on the risks' inherent qualities (regulatory, technological) and levels on which they exert their effect, without clearly delineating the difference between internal and external forces affecting project risk (strategic, operational). This method is plainly inadequate because it does not adequately depict risks that may occur with other stakeholders and their systems, as the PCS is a system that is connected to many other systems. These hazards that arise in the project's environment are frequently overlooked, yet they have a significant impact on the project execution. The following sources of risk in form of the residual risk were not identified, but had impact on the project until the completion:

1. In the production system, data flow and message exchange between PCS and MNSW CIMIS must be synchronized, as CIMIS does not provide for an up-to-date test environment.

2. As the functional definition and development are in the early phases, there is a possibility of not being able to provide modules D8 and D9 for concessionaire Port of Rijeka, j.s.c., until the determined end of the project.

3. There are multiple parallel project activities and module developments, putting pressure on the supplier's capabilities and endangering module completion and integration, as well as ultimate product quality. This inherent risk is also reduced by the project's prolongation.

4. Given that the comprehensive transition of module D3 to production necessitates additional comprehensive testing, the deadline for the transition of this module to production can be more easily adjusted to the new framework of the final contract extension, considering the concessionaire's and other stakeholders' availability.

5. The risk of module D10 development has been carried forward to the start of production. The project's extension allows for the implementation of the D10 module. It will be necessary to achieve an agreement on whether the concessionaire will allow D3 module production without CFS or insist on simultaneous production of both modules. Because the deadline for continued collaboration on the CFS module's integration with PCS, as well as the expected timeframe for its transfer to production, is uncertain whether the D10-CFS module will be implemented prior to the end of Q4 2022.

6. Customs office has not yet taken a decision on whether or not to keep control lists in the customs system, and the PCS continues to function under present regulations, which means that control lists previously established in the customs IT system will be manually inserted into the PCS system. These features were successfully evaluated as part of module D3's rigorous internal User Acceptance testing.

7. Customs services for NCTS and HRAIS are currently being developed. Although PCS can function without these services, MRN services cannot. They will work with the latest versions of NCTS5 [19] and HRAIS2 [20].

Therefore, it was apparent that the enterprise risk management approach did not clearly identify all barriers, drivers, and success factors of the PCS development.

V. Conclusion

Internal and external stakeholders were involved in the process of building a national PCS model in Croatia, including the subject Ministry, Port Authority, integration and development services provider, and technical assistance team, as well as concessionaires, customs, police, port captains, ship and cargo agents, port control centre, and various digital systems that will exchange data with the new PCS. Under the auspices of the CEF EU financing, a project was launched in Croatia in mid-2017 to begin the construction of a national model of Port Community System, which was initially deployed in the Port of Rijeka and began production work in early 2022. The Port Community System, a digital platform for exchanging cargo messages and data among the port cluster's many stakeholders, should be adopted in other Croatian cargo ports in the near future.

The project's execution was substantially influenced by the recognized and residual risk. While the traditional strategy was effective for managing and treating recognized risk, it was insufficient for reducing residual risk to a minimal feasible level. The fact that the final risk identification revealed a more thorough risk occurrence registry, as well as additional drivers, success factors, and obstacles, clearly demonstrates this fact. The supplier proposed project risk management, which was handled in the same way as the traditional enterprise risk management. The project risk was broken down into numerous areas, including strategic, operational, technological, and regulatory aspects, with risk likelihood, impact, and mitigation strategies identified. This approach is appropriate for projects and environments where categorical risk is high (for example, caused by the complexity of the used hardware, network, and system support), but it lacks refinement in situations where multiple stakeholders operate their own information systems that must be integrated and communicate with the PCS.

These environments are often external to the PCS and contain undisclosed disk categories that are difficult to prepare ahead of time, as those planning and administering the project typically have very limited visibility of these complicated external systems and much less options for mitigation at the time of their occurrence. The use of the described approach in analysing and reengineering of additional processes (mostly commercial processes, not administrative processes) associated to the introduction of integral business information systems best suited for seaport clusters might lead to further study.

REFERENCES

[1] Port Authority Rijeka, European projects, CEF – POR2CORE – PCS [Online]. Available: https://www.portauthority.hr/europskiprojekti/975/.

[2] Republic of Croatia, Ministry of the Sea, transport and Infrastructure, CIMIS – Croatian Integrated Maritime Information System [Online]. Available: https://mmpi.gov.hr/more-86/vts-croatia-114/cimis-hrvatski-integriranipomorski-informacijski-sustav/16553.

[3] The European Union, European Commission, The Innovation and Networks Executive Agency (INEA) [Online]. Available: https://ec.europa.eu/inea/en/welcome-to-innovation-networksexecutive-agency.

[4] The European Union, European Commission, Connecting Europe Facility, CEF Transport, Upgrade of the Rijeka Port infrastructure – Port Community System (POR2CORE-PCS) [Online]. Available: https://ec.europa.eu/inea/en/connectingeurope-facility/cef-transport/2016-hr-tmc-0082-s.

[5] Republic of Croatia, Ministry of the Sea, transport and Infrastructure [Online]. Available: https://mmpi.gov.hr/en.

[6] World Customs Organization, Building a single window environment, Compendium V.1, 2020 [Online]. Available: http://www.wcoomd.org//media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/single-window/compendium/swcompendiumvol1all-parts.pdf.

[7] Kapidani, N., Tijan, E., Jović, M. and Kočan, E. (2020) "National Maritime Single Window – Cost-Benefit Analysis of Montenegro Case Study", Promet – Traffic&Transportation, 32(4), pp. 543-557. doi: 10.7307/ptt.v32i4.3422.

[8] Interreg Italy-Croatia Transpogood project, Drivers and Barriers identification, Final Version of 20/09/2019., Deliverable Number: D.5.1.1. [Online]. Available: https://www.italycroatia.eu/documents/120312/1577990/D5.1.1.+Drivers+and+Barriers+identification.pdf/f0579b91-b7ba-32af-01bdcce7dd67caa7?t=1591009546900

[9] Dr. Nils Meyer-Larsen, Project Manager, The Institute of Shipping Economics and Logistics (ISL), Better Cybersecurity for Port Community Systems, Edition 76: winter 2017., PTI Edition 76: Cyber Risk & Security [Online]. Available: https://www.porttechnology.org/editions/cyber_risk_security/

[10] Republic of Croatia, Ministry of Finance, Customs Administration, e-Customs [Online]. Available: https://carina.gov.hr/e-customs/6678

[11] Actual I.T. d.d., Funkcionalna specifikacija: PORT2CORE PCS ICT sustav, version 8.0, Port Community System 2020., 2021.

[12] First annex to the contract nr. 1 11-18 L.U. for delivery and installation of the PCS system, Rijeka, Croatia, 4th May 2020.

[13] Second annex to the contract nr. 1 11-18 L.U. for delivery and installation of the PCS system, 26th November 2020., Rijeka, Croatia

[14] Third annex to the contract nr. 1 11-18 L.U. for delivery and installation of the PCS system, 29th December 2021., Rijeka, Croatia

[15] Port Authority Rijeka, Port Control Centre [Online]. Available: https://www.portauthority.hr/en/rijeka-traffic-24-h-port-control centre/

[16] The public procurement portal of the Republic of Croatia „Narodne novine", Port Authority Rijeka, Delivery and installation of PCS systems [Online]. Available: https://eojn.nn.hr/SPIN/APPLICATION/IPN/DocumentManagement/DokumentPodaciFrm.aspx?id=5912617

[17] Gregg Witte, Huntington Ingalls Industries Inc., „Implementing an enterprise risk management framework", 12.10.2021., TechTarget [Online]. Available: https://www.techtarget.com/searchcio/feature/Implementing-an enterprise-risk-management-framework

[18] Goodman, R. (2005). The ascent of risk: risk and the Guide to the project management body of knowledge (PMBOK guide), 1987 1996-2000-2004. Paper presented at PMI® Global Congress 2005—Asia Pacific, Singapore. Newtown Square, PA: Project Management Institute [Online]. Available: https://www.pmi.org/learning/library/ascent-risk-pmbokguide7618

[19] Republic of Croatia, Ministry of Finance, Customs Administration, NCTS phase 5 [Online]. Available: https://carina.gov.hr/istaknute-teme/e-carina/ncts-faza-5/9845

[20] Republic of Croatia, Ministry of Finance, Customs Administration, HRAIS2 [Online]. Available: https://carina.gov.hr/istaknute-teme/e-carina/hrais2/8267