Resilience in Law Enforcement Technology Design and Development: Analysing user requirements for current approaches in European border security research and innovation

Laura Salmela
Kirsi Aaltola
Sirra Toivonen
Santtu Lehtinen
VTT Technical Research Centre of Finland

Abstract

The COVID-19 pandemic has accentuated the meaning of resilience for European digital infrastructures which safeguard vital societal functions, such as the activities of European law enforcement authorities. The pandemic has vividly illustrated that unreliable IT-systems and networks cripple also authorities' business continuity and access to critical information when alternative processing methods remain scarce during times of transformed social interaction. The development of resilience thus demands research and innovation investments also in the future, as emerging risks, both physical and human-made, may produce long-lasting consequences to systems critical to European safety and security. In EU-funded security research, resilience has formed a well-established concept even before current events and prolonged crisis, however, not uniformly across all law enforcement domains. This article focuses on border security research in the H2020 programme and analyses how resilience is addressed within this field. The H2020 programme underlines practitioners' decisive role in determining the requirements for future technological solutions. Therefore, we concentrate on the initial stages of the systems design and development process, in particular the user requirements elicitation phase. The article's specific aims are to identify preliminary resilience perspectives, which users convey forward in the design and development process, and propose future research directions to strengthen resilience thinking also in the border security domain.

Keywords: *Research and Innovation, Border Security, Resilience, Human-Centred Design, User Requirements*

Introduction

The COVID-19 pandemic has challenged and thoroughly tested the resilience of European digital infrastructures which maintain and support vital societal functions, such as the operations, daily tasks and processes of different law enforcement authorities (LEA) in EU Member States. In the area of EU's Justice and Home Affairs (JHA), a prolonged period of social distancing visibly demonstrates the high reliance of actors and organisations on digital technologies in terms of access to information, business continuity and availability of critical IT-systems and underscores the technologies' pivotal role in safeguarding LEA core functions, particularly from the perspective of societal resilience (eu-LISA, 2020). As the pandemic limits society's abilities to resort to alternative processes, expectations towards the dependability of IT-systems in delivering reliable services increase. EU's new Cybersecurity Strategy and the European Commission's proposal for a new directive prioritise the position of resilience within European policies related to critical entities and networks (European Commission, 2020a). Effective adaptation to potentially long-lasting consequences of new risks requires further development of resilience in decisive systems.

Even before the ascent of the current pandemic and renewed policies, resilience enjoyed an accentuated position in EU-funded security research that aims to support and improve the capabilities of governmental organisations working towards societal safety and security in Europe. In the Horizon 2020 (H2020) Research and Innovation Programme of the European Union (2014-2020), resilience has formed a central concept for research activities particularly related to the protection of critical infrastructure, the development of Artificial Intelligence (AI) technologies, disaster management and digital security, and novel technologies constitute one key means to enhance the resilience of critical systems (European Commission, 2020b). However, besides significant benefits, new technologies may predispose critical systems to novel risks that have also the potential to cascade, particularly in highly networked and interdependent societies (Linkov & Palma-Oliveira, 2017).

Since the start of the millennium, digitalisation has significantly transformed European border management not only in authorities' back-end processes but also at the level of equipment, tools, and systems implemented to the monitoring and controlling of EU's external borders and the cross-border flow of persons, goods, vehicles and vessels. Initiatives to enhance digitalisation and harmonisation of practices at borders were established already a decade ago (more on 'Smart Borders' policy, see for example Lehtonen & Aalto, 2017; Jeandezboz, 2016), and system interoperability together with innovative technologies increasingly form the cornerstones of border authority capabilities against emerging risks. These developments argue for a more holistic assessment of the ways in which novel border security technologies tolerate, recover and adapt to foreseen or unforeseen changes during their expected service life. According to Linkov & Palma-Oliveira (2017), resilience-based approaches enable the assessment of system capabilities needed to ensure dynamic adjustment to various transformations that affect systems negatively. Nevertheless, border security research calls address resilience primarily from a societal perspective (European Commission, 2020b), while explicit requirements towards improving the physical and digital resilience of a system are less-documented. Overall, focus "on the (technical) resilience of smaller systems" (Häring et al., 2017: 23) remains scarce; a characterisation which may also apply to border security research.

The primary objective of this article is to examine the manifestation of resilience approaches in the H2020 border security research. Border security interfaces and integrates with the law enforcement domain at different levels for example through institutional and organisational ties (Center for the Study of Democracy, 2011) and approaches to harmonise LEA training and crisis management within Europe and beyond (Frontex, 2020; Taitto & Hyttinen, 2018). The H2020 programme highlights active participation of security practitioners in research, and assigns key end-users a significant role in defining and establishing the requirements for future technological solutions (see for example European Commission 2015a, 2017, 2020b). As a result, we concentrate on the initial stages of the systems design and development process and analyse the ways in which the user needs elicitation phase acknowledges system resilience attributes. The article's specific aims are to identify preliminary resilience perspectives, which users convey forward in the design and development process, and propose future research directions to strengthen resilience thinking also in the border security field.

Theoretical points of departure

Engineering systems and resilience

Constructing resilient systems is a challenge that systems engineering pursues to answer both as a scientific discipline and as a pragmatic activity. Fortifying resilience in complex systems constitutes an increasingly important task due to the dynamic nature of emerging risks and threats that overburden systems (Small et al., 2018). Engineering resilience is not only about building-in resilience through certain techniques, but also about ensuring ways in which the resilience of a system can be maintained or managed in the long run (Hollnagel, 2010a).

The definition of resilience depends on its application context, use incentive or research discipline to a large degree (Curt & Tacnet, 2018; Park, 2011; Uday & Marais, 2019). Infrastructure research defines system resilience for example as follows:

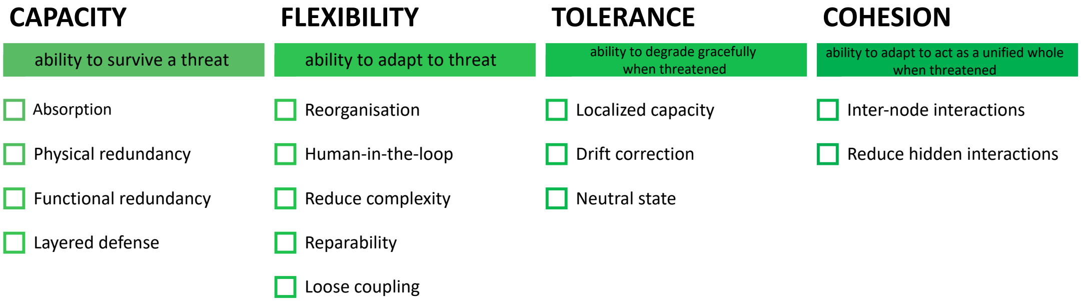
"Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance" (Vugrin, 2010: 83).

Another definition proposes that resilience is "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" (Hollnagel, 2010b: xxxvi). Resilience research tends to oppose a static view on system capabilities but claims them being susceptible to temporal alterations that originate from system performance and capacity variations transpiring in different time periods (Linkov & Palma-Oliveira, 2017).

Certain qualities can be said to characterise a resilient system. For example, Hollnagel (2010: xxix) establishes that a resilient system has to possess the four following abilities: "the ability to respond to events, to monitor ongoing developments, to anticipate future threats and opportunities, and, to learn from past failures and successes alike". Particular system capacities, either endogenous (internal) or exogenous (external), are also applied to define resilience. First, absorptive system capacity relates to "the degree to which a system can automatically absorb the impacts of system perturbations and minimize consequences with little effort". Adaptive system capacity on the other hand refers to "the degree to which the system is capable of self-organisation for recovery of system performance levels", while restorative capacity is "the ability of a system to be repaired easily". (Vugrin, 2010: 99-101) In contrast to engineering fail-safe systems, an objective of 'traditional risk analysis', resilience management emphasizes the construction of systems that exhibit flexibility and adaptive capabilities to function in new circumstances arising after adverse events. Resilience management thus aspires to ensure that adverse events do not permanently deteriorate a system's functions and performance. The time horizon for resilience management expands that of risk management. (Linkov & Palma-Oliveira, 2017)

With regards to design principles, Jackson and Ferris (2013) propose a taxonomy of 14 principles organized into four attributes guiding the engineering of resilient systems. Figure 1 defines the attributes (capacity, flexibility, tolerance, cohesion) and lists related design principles under each attribute.

Figure 1. Taxonomy of resilience for engineered systems. Reproduced and modified from Jackson & Ferris 2013, p. 155



CAPACITY	FLEXIBILITY	TOLERANCE	COHESION
ability to survive a threat	ability to adapt to threat	ability to degrade gracefully when threatened	ability to adapt to act as a unified whole when threatened
☐ Absorption	☐ Reorganisation	☐ Localized capacity	☐ Inter-node interactions
☐ Physical redundancy	☐ Human-in-the-loop	☐ Drift correction	☐ Reduce hidden interactions
☐ Functional redundancy	☐ Reduce complexity	☐ Neutral state	
☐ Layered defense	☐ Reparability		
	☐ Loose coupling		

Research and innovation projects accentuate also other desirable system qualities than only resilience, such as performance, productivity, compatibility with adjacent systems or compliance with legal and ethical requirements. The primary objectives of European border security research demonstrate this by emphasizing the need "to enhance systems and their interoperability, equipment, tools, processes, and methods for rapid identification to improve border security, whilst respecting fundamental rights including free movement of persons, protection of personal data, and privacy" (European Commission, 2020b: 14).

Project objectives often question the feasibility or suitability of all resilience principles for a single system, as trade-offs may need to be made within them, such as whether to implement high physical or functional redundancy at the cost of achieving less complex designs (Jackson & Ferris, 2013). In addition, resilience requirements exhibit interdependence (Jackson & Ferris, 2013), and complement or overlap with other important system properties (Firesmith, 2020). In general, research tends to contradict in whether resilience requirements form a specific requirement group and clearly differ from system requirements that relate to other quality attributes, such as robustness, safety, cybersecurity, or anti-tamper (Firesmith, 2020). Furthermore, some system attributes are considered to "enable systems to achieve resiliency", such as adaptability, extensibility, flexibility, repairability and versatility (Enos, 2019: 389-390).

User involvement in system design processes

Several studies, addressing different contexts and fields, highlight the value and contribution of user or human involvement in technology design and development (see for example Leikas, 2009; Kujala et al., 2005; Karvonen & Martio, 2018; Niemelä et al., 2014; Aaltola, 2021; Aaltola, 2020). User involvement is claimed to enhance system usability, usefulness, user satisfaction and overall success (Kujala et al., 2005), and breed innovations in product development processes through direct interaction via interviews or through observation of user behaviour in real-life use situations and contexts (Dell'era & Landoni, 2014). Users fill an important knowledge gap, as assuming the role of an inexperienced user is considered unattainable for developers (Wallach & Scholz, 2012). Despite multiple benefits associated with human centricity of design, research also reports various challenges pertaining to the role of users in related processes and particularly emphasizes the importance of scientific or evidence-based information to which design decisions need to be grounded (Saariluoma, 2005; Reymen, Whyte & Dorst, 2005; Luck, 2003).

In the H2020 funding programme, project eligibility and admissibility conditions formalise the involvement of practitioners or user representatives at the very general level in certain topics, particularly those related to security research (see for example European Commission 2020b). This conforms to the lessons learned from the preceding Framework Programme 7 that demanded "more active end-user participation" in future programmes (European Commission, 2015b: 72). For example in border security related sub-topics, the eligibility and admissibility conditions require projects to actively engage a minimum of three EU Member State or Associates Countries' authorities (European Commission, 2020b). The elementary reason to design and develop technology also applies to security research; technology can and should essentially improve the quality of life (Saariluoma, Cañas & Leikas, 2016). Involving users thus enhances the understanding of what technology could actually offer for people in practice, and in what forms or under what terms it would be welcomed and adopted efficiently.

Data collection and analysis in brief

For the purpose of this paper, we reviewed all on-going and closed H2020 Border and External Security (BES)-projects under the action types of Research and Innovation Action (RIA) and Innovation Action (IA). The collection of project data in the Community Research and Development Information Service (CORDIS) repository revealed that 25 BES-projects are or have been financed since the start of the H2020 programme until October 2020. However, the final selection of projects reduced to six (6) as only these projects grant access to deliverables concerning user needs and requirements. During the research, it became clear that in most of the projects, user needs or requirements related deliverables have been assigned a dissemination level Confidential or EU RESTRICTED which limits project documentation availability. Figure 2 presents a list of the examined projects.

Figure 2. List of analysed projects. The projects may be categorised at the general level in terms of context-relevant focus: border checks, border surveillance and examination of prospective migrants' perceptions of Europe

PROTECT	SMILE	PERSONA	CAMELOT	MARISA	MIRROR
□ Theme: Border Checks	□ Theme: Border Checks	□ Theme: Border Checks	□ Theme: Border Surveillance	□ Theme: Border Surveillance	□ Theme: Migration
□ Project Type: RIA	□ Project Type: RIA	□ Project Type: RIA	□ Project Type: IA	□ Project Type: IA	□ Project Type: RIA
□ Duration: 2016-2019	□ Duration: 2017-2020	□ Duration: 2018-2021	□ Duration: 2017-2021	□ Duration: 2017-2020	□ Duration: 2019-2022

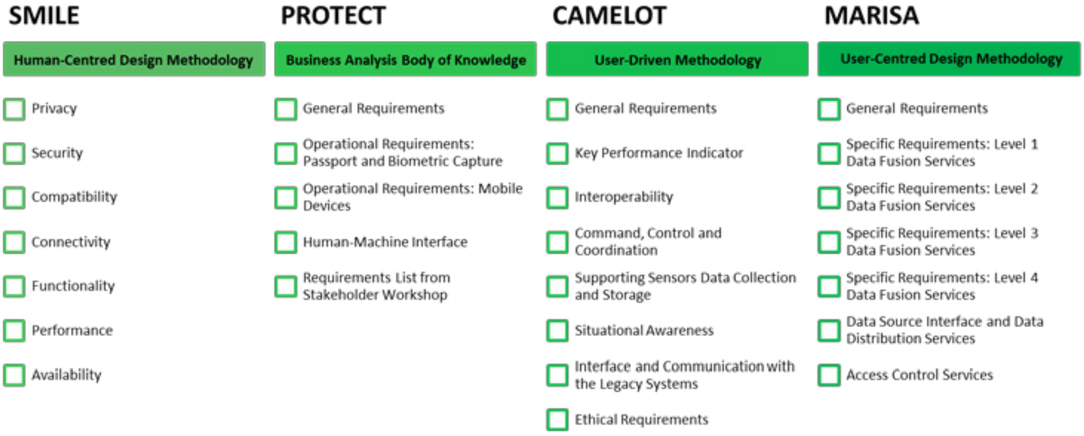
The projects identify and analyse user needs and user requirements. As the distinction between the terms is ill-defined, we apply user needs and user requirements interchangeably in this paper. Overall, most projects include a user needs analysis task in their work, and the projects seem to be structured according to standard systems development processes (for example the V-model by Clark, 2009), in which user requirements are identified and specified at the beginning and validated towards the end of a project. Projects implement partially differing reporting methods for user requirements. Some projects produce several versions of user requirements documents, while others specify requirements in a single deliverable.

Following the desk study consisting of empirical data collection, we conducted a comparative analysis between the selected projects' user requirements. Firstly, we examined and compared the applied methodologies for user needs elicitation with the aim of seeking potential areas of similarity or difference between the projects. Secondly, we studied how the requirements were structured and categorised to identify reoccurring system quality attributes. Finally, we investigated how resilience-relevant user requirements are analysed and reported. As resilience has not been in focus in the H2020 border security research projects, it was not assumed that resilience would strongly surface from the projects' research outputs and in their overall technology development. Thus, we investigated whether the requirements address relevant capabilities or features that enable systems to efficiently resist, recover and adapt to the effects of events which negatively influence a system's critical functions for certain a time period or indefinitely.

User requirements approaches in projects and the identification of resilience requirements

The examined projects tend to emphasize a human-centred, user-centred, or user-driven approach towards requirements specification and system design. Key standards or established business practices, such as the ISO 9241 series on ergonomics of human system interaction (revising former ISO 13407 series) or the Business Analysis Body of Knowledge ('the BABOK Guide'), constitute the methodological foundations of the selected design approaches. The projects implement the main principles of human-centred design (International Standardisation Organisation, 2019) for example by 1) gathering information and describing in detail future system users and the envisioned implementation environments; 2) engaging users to different phases of system design and development; 3) emphasizing the role of users in the evaluation of project outputs; and 4) applying an iterative process to specify requirements. The projects employ various research methods to each principle for example with regards to how the user requirements are identified or prioritised. In itself, user requirements specification forms one important activity in human-centred design with the aim "to create an explicit statement of user requirements in relation to the intended context of use and the business objectives of the system" (International Standardisation Organisation, 2019: 13). Project documentation (i.e. analysed deliverables) can be understood as that explicit statement of user requirements specified for the objectives of a particular project. The finalised requirements demonstrate key discrepancies, despite the projects share the same methodologies for the overall design and development process. Particularly, the projects typify and cluster user requirements differently. Figure 3 summarises the main methodologies and user requirements classifications in an example set of projects.

Figure 3. Implemented methodologies and requirement classification in four projects



SMILE

Human-Centred Design Methodology

□ Privacy
□ Security
□ Compatibility
□ Connectivity
□ Functionality
□ Performance
□ Availability

PROTECT

Business Analysis Body of Knowledge

□ General Requirements
□ Operational Requirements: Passport and Biometric Capture
□ Operational Requirements: Mobile Devices
□ Human-Machine Interface
□ Requirements List from Stakeholder Workshop

CAMELOT

User-Driven Methodology

□ General Requirements
□ Key Performance Indicator
□ Interoperability
□ Command, Control and Coordination
□ Supporting Sensors Data Collection and Storage
□ Situational Awareness
□ Interface and Communication with the Legacy Systems
□ Ethical Requirements

MARISA

User-Centred Design Methodology

□ General Requirements
□ Specific Requirements: Level 1 Data Fusion Services
□ Specific Requirements: Level 2 Data Fusion Services
□ Specific Requirements: Level 3 Data Fusion Services
□ Specific Requirements: Level 4 Data Fusion Services
□ Data Source Interface and Data Distribution Services
□ Access Control Services

Our analysis indicates that human-centred design poorly guides towards harmonised classification of user requirements after their identification and specification have been performed. On the contrary, the classification appears project-dependent and originates 1) bottom-up from the requirements identification and analysis process, 2) top-down from the system and its envisioned functions or other important aspects being developed in the project, or 3) their mixture. Together with the main requirement classes, the projects typify user requirements into functional and non-functional requirements. Functional requirements refer to "what the product has to do, the rules that it has to carry out or what processing actions it must take", while non-functional requirements describe "the properties that the functions must have, such as performance and usability" (Atlantic Systems Guild Limited, 2016: 7). However, some projects perform this kind of classification at a next stage of the requirements engineering process, in which user requirements are developed into system requirements (a requirement type that is distinctive from but related to a user requirement). Overall, the projects tend to lack consistency in the requirements classification into functional and non-functional, if one reflects individual requirement specifications against definitions proposed by the requirements engineering literature.

Our analysis of the project outputs at the classification level shows that the concept of resilience manifests weakly in the user requirements data. Resilience does not form an explicit primary or secondary requirement class, or a visible system quality attribute as presented in the theoretical section of this article. Overall, the analysed materials lack a definition for resilience and cover the terms resilience, resilient, or resiliency in a limited way. Identifying distinctive resilience requirements from the set of user requirements thus becomes unfeasible.

Nevertheless, certain requirement classes may indicate a relation to resilience, such as availability or security. A requirement may establish that a 24/7 access to the system must be guaranteed (SMILE, 2019) or the data transmission and overall communication must be secured (SMILE, 2019; PERSONA, 2019). Also, certain requirements typified under so-called general requirements can be relevant for developing system resilience. An individual requirement may establish for example that the system “must work continuously without critical failures, regardless of weather conditions (clear, fog, rain, thunderstorms) or time of day (dawn, day, dusk, night)” (CAMELOT, 2018: 44) or it “shall guarantee high availability (e.g. MTBF 10.000 hours without major faults compromizing the continuation of the nominal mission) of data and services” (MARISA, 2019: 30).

Although traits of resilience can be detected in some user requirements, presenting these as distinctive resilience requirements involves a great deal of interpretation and requires further analysis of project objectives and other information. This may eventually erode the reliability of such analysis, as individual researchers may arrive at alternative interpretations. However, what this paper does suggest is that users indeed emphasize the importance of resilience-relevant system properties, as users conveyed such needs in the needs identification process. Nevertheless, the current analysis cannot ascertain whether the users expressed these needs or requirements for the purpose of designing a *resilient* border security system from a physical, digital, or other perspective. Resilience requirements, if interpreted as such, appear mostly in a scattered form across the project materials.

Concluding remarks and future outlook

In the Justice and Home Affairs domain, policy demands and grass-roots level development needs accentuate the growing importance of digital infrastructure resilience. As the role of technology in LEA operations expands, and the implemented systems increase in complexity with direct human-in-the-loop possibilities subsiding, questions relating to the necessity of resilience and its design into critical systems become even more topical (see for example Uday & Marais, 2015). Still, to make resilience truly actionable, there is an apparent need for "a definition and an explanation of an observable, measurable system attribute" to avoid resilience remaining "a vague concept rather than a practical policy or management tool" (Fekete et al., 2014: 5). As the JHA community seems to lack a shared definition for digital resilience (eu-LISA, 2020), substantial work lies ahead to ensure an efficient exploitation of lessons learned and avoidance of prior pitfalls experienced in other domains. For border security risk analysis, shared models and frameworks have already been developed at the European level (Frontex, 2013), and research initiatives on risk-based approaches towards border management are progressing (for example the TRESSPASS project http://www.trespass-project.eu/).

In this paper, we examined how resilience is addressed in contemporary border management – a distinctive activity in law enforcement. We focused our examination to border security research within the H2020 programme and narrowed our analysis to particular activities in system design and development processes within a selected set of projects. To bridge the gap between broad policy objectives of resilience and border security operations at the practitioner level, we scrutinized how resilience currently manifests in the needs and requirements established by prospective users of future innovative technologies. Identification and specification of user requirements comprise one means to understand what users expect and demand from new systems and tools.

The results of this study indicate that resilience is an underused design principle, a concept (resilience-by-design) or an aspired system quality attribute in the current border security research. Relevant requirement classes and individual requirements may be identified in the set of requirements, however, the reliability of this interpretation can be challenged as no explicit references to resilience are made. Our analysis concludes that the projects' main objectives are situated elsewhere than in resilience, and the primary resilience qualities as defined for example by Jackson & Ferris (2013) do not strongly drive the projects' design and development process, at least in the initial phases. New solutions are developed to provide border management authorities with efficient tools against known and emerging risks and threats, such as terrorism, piracy, cybercrime, and diverse kinds of fraud. However, research initiatives promoting for example the development of absorptive, adaptive or restorative system capacities (Vugrin, 2010) against a suite of different physical and digital risks, both natural and human-made, are still limited. This might also prompt for a more systems theory based approach, since resilience can be understood as an emergent system property which cannot be reduced to lower level system capabilities that individual components might provide (see for example Leveson, 2012).

Although the current examination yielded compelling results, the limitations of our work need to be acknowledged as well. Due to restricted access to materials, we examined only a part of all H2020 research projects in the Border and External Security topic. As border management systems are highly security-critical infrastructures contributing to the national security of EU member states and EU's internal security as a whole, threat, vulnerability and capability assessments or related scenarios remain mostly confidential (see for example European Commission, 2020c). Additionally, within the examined six research projects, we focused our inquiries only on a limited set of project outputs and documentation that relate to specific tasks and parts of the projects' work. Somewhat heterogeneous methods and practices applied in the analysed projects challenged a meaningful cross-comparison of project outputs, as coinciding data were difficult to identify. As other safety and security specific H2020 topics (e.g. disaster management) concentrate more on resilience, a comparative analysis between border security research and the aforementioned fields could substantiate our findings and provide added value in developing suitable resilience approaches also for border security purposes. Moreover, it might provide better understanding how user involvement can be utilised in the engineering of resilient systems. Without achieving "a universal understanding of resilience" (Francis & Bekera, 2014: 92) within the JHA community or border security for that matter, it can be difficult for users even to express needs and requirements for such a system, if the concept remains elusive in its meaning.

References

- Aaltola K. (2021) Empirical study on cyber range capabilities, interactions and learning features. In: Tagarev T., Atanassov K.T., Kharchenko V. & Kacprzyk J. (eds.) *Digital transformation, cyber security and resilience of modern societies*. Studies in Big Data, vol 84. Springer, Cham, pp. 413-428.
  Available from: https://doi.org/10.1007/978-3-030-65722-2_26
- Aaltola, K. (2020) New technologies shaping learning?: AR learning experiences and integration model. In: Zheng, R. (ed.) *Cognitive and Affective Perspectives on Immersive Technology in Education*. IGI Global, pp. 195-214.
  Available from: https://doi.org/10.4018/978-1-7998-3250-8.ch010
- Atlantic Systems Guild Limited (2016) Volere Requirements Specification Template Edition 18—2016.
- CAMELOT project (2018) *D2.1 User requirements and use cases*.
  Available from: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bfa8f1e9&appId=PPGMS [Accessed 30th March 2021].
- Center for the Study of Democracy (2011) *Better management of EU borders through cooperation. Study to identify best practices on the cooperation between border guards and customs administrations working at the external borders of the EU*.
  Available from: https://ec.europa.eu/home-affairs/sites/default/files/e-library/docs/pdf/customs_bgs_final_en.pdf [Accessed 30th March 2021].

- Clark, J. O. (2009) System of systems engineering and family of systems engineering from a standards, V-model, and dual-V model perspective. *3rd Annual IEEE Systems Conference, Vancouver, BC, Canada, 23-26 March, 2009*. pp. 381-387.
Available from: 10.1109/SYSTEMS.2009.4815831

- Curt, C. & Tacnet, J. (2018) Resilience of critical infrastructures: review and analysis of current approaches. *Risk Analysis*. 38 (11), 2441-2458.
Available from: https://doi.org/10.1111/risa.13166

- Dell'Era, C. & Landoni, P. (2014) Living Lab: A methodology between user-centred design and participatory design. *Creativity and Innovation Management*. 23 (2), 137-154.
Available from: https://doi.org/10.1111/caim.12061

- Enos, J. (2019) Achieving resiliency in major defense programs through non-functional attributes. *Systems Engineering*. 22, 389-400.
Available from: https://doi.org/10.1002/sys.21488

- eu-LISA (2020) *Interoperability – building digital resilience for the eu justice and home affairs community*. 7th Annual Conference, 26 November 2020, Online.
Available from: https://www.eulisaconference.eu/report-2020/ [Accessed 30th March 2021].

- European Commission (2015a) *Horizon 2020 Work Programme 2014 – 2015 14. Secure societies – Protecting freedom and security of Europe and its citizens. Revised.*
Available from: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-security_en.pdf [Accessed 1st December 2020].

- European Commission (2015b) *Final evaluation of security research under the seventh framework programme for research, technological development and demonstration - Final Report*.
Available from: https://op.europa.eu/en/publication-detail/-/publication/1054a8af-8389-11e5-b8b7-01aa75ed71a1/language-en/format-PDF/source-search [Accessed 1st December 2020].

- European Commission (2017) *Horizon 2020 Work Programme 2016 – 2017 14. Secure societies – Protecting freedom and security of Europe and its citizens.*
Available from: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf [Accessed 1st December 2020].

- European Commission (2020a) *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*. Press release. 16th December 2020.
Available from: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 [Accessed 16th March 2021].

- European Commission (2020b) *Horizon 2020 Work Programme 2018-2020. 14. Secure societies - Protecting freedom and security of Europe and its citizens*.
Available from: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf [Accessed 1st December 2020].

- European Commission (2020c) *Horizon 2020 Programme. Guidance. Guidelines for the classification of information in research projects*.
Available from: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/secur/h2020-hi-guide-classif_en.pdf [Accessed 16th March 2021].

- Firesmith, D. (2020) *System resilience part 3: engineering system resilience requirements*. Software Institute Engineering Blog, 13th Jan 2020.
Available from: https://insights.sei.cmu.edu/sei_blog/2020/01/engineering-system-resilience-requirements.html [Accessed 16th March 2021].

- Francis, R. & Bekera, B. (2014) A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering and System Safety*. 121, 90-103.
Available from: https://doi.org/10.1016/j.ress.2013.07.004

- Frontex (2013) *Common Integrated Risk Analysis Model*. Summary booklet.
  Available from: https://frontex.europa.eu/assets/CIRAM/en_CIRAM_brochure_2013.pdf [Accessed 30th March 2021].

- Frontex (2020) *Frontex signs working arrangement with CEPOL*. News Release, 20th October 2010.
  Available from: https://frontex.europa.eu/media-centre/news/news-release/frontex-signs-working-arrangement-with-cepol-EVYGrV [Accessed 30th March 2021].

- Hollnagel, E. (2010a) Epilogue: RAG – the Resilience Analysis Grid. In: Pariès, J. & Wreathall, J. (eds.) *Resilience Engineering in Practice: A Guidebook*. Farnham: Taylor & Francis Group. pp. 275-296.
  Available from: ProQuest Ebook Central. [Accessed 30 March 2021].

- Hollnagel, E. (2010b) Prologue: The scope of resilience engineering. In: Pariès, J. & Wreathall, J. (eds.) *Resilience Engineering in Practice : A Guidebook*. Farnham: Taylor & Francis Group. pp. xxix-xxxix.
  Available from: ProQuest Ebook Central. [Accessed 30 March 2021].

- Häring, I., Sansavini, G., Bellini, E., Martyn, N., Kovalenko, T., Kitsak, M., Vogelbacker, G., Ross, K., Bergerhausen, U., Barker, K. & Linkov, I (2017) Towards a generic resilience management, quantification and development process: general definitions, requirements, methods, techniques and measures, and case studies. In: Linkov, I. & Palma-Oliveira, J. M. (eds.) *Resilience and Risk. Methods and Application in Environment, Cyber and Social Domains*. NATO Science for Peace and Security Series - C: Environmental Security. Dordrecht, The Netherlands, Springer, pp. 21-80.

- International Standardisation Organisation (2019) *ISO 9241-210:2019 Ergonomics of human-system interaction. Part 210: Human-centred design for interactive systems.* Geneva, ISO.

- Jackson, S. & Ferris, T. (2013) Resilience principles for engineered systems. *Systems Engineering*. 16 (2), 152-164.
  Available from: https://doi.org/10.1002/sys.21228

- Jeandesboz J. (2016) Smartening border security in the European Union: An associational inquiry. *Security Dialogue*. 47 (4), 292-309.
  Available from: https://doi.org/10.1177/0967010616650226

- Karvonen, H. & Martio, J. (2018) *Human factors issues in maritime autonomous surface ship systems development*. In: Lee, K. & Rødseth, Ø. J. (eds.) *Proceedings of the 1st International Conference on Maritime Autonomous Surface Ships, ICMASS 2018, 8-9 November 2018, Busan, Republic of Korea*. SINTEF Academic Press. pp. 35-40.
  Available from: http://hdl.handle.net/11250/2599019 [Accessed 30 March 2021].

- Kujala, S., Kauppinen, M., Lehtola, L., Kojo, T. (2005) *The role of user involvement in requirements quality and project success*. In: *Proceedings of the 2005 13th IEEE International Conference on Requirements Engineering (RE'05), 29 August – 2 September 2005, Paris, France*. IEEE Computer Society.
  Available from: https://doi.org/10.1109/RE.2005.72

- Lehtonen, P. & Aalto, P. (2017) Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States. *European Security*. 26 (2), 207-225.
  Available from: https://doi.org/10.1080/09662839.2016.1276057

- Leikas, J. (2009) *Life-based design. A holistic approach to designing human technology interaction*. Espoo, VTT Technical Research Centre of Finland.
  Available from: https://www.vttresearch.com/sites/default/files/pdf/publications/2009/P726.pdf [Accessed 30 March 2021].

- Linkov, I. & Palma-Oliveira, J.M. (2017) An introduction to resilience for critical infrastructures. In: Linkov, I. & Palma-Oliveira, J. M. (eds.) *Resilience and Risk. Methods and Application in Environment, Cyber and Social Domains*. NATO Science for Peace and Security Series - C: Environmental Security. Dordrecht, The Netherlands, Springer. pp. 3-17.

- Luck, R. (2003) Dialogue in participatory design. *Design studies*, 24(6), 523-535.
  Available from: https://doi.org/10.1016/S0142-694X(03)00040-1

- MARISA project (2019) *D2.9 MARISA user requirements (Final)*.
  Available from: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c2790526&appId=PPGMS [Accessed 30 March 2021].

- Niemelä, M., Ikonen, V., Leikas, J., Kantola, K., Kulju, M., Tammela, A., & Ylikauppila, M. (2014). Human-driven design: a human-driven approach to the design of technology. In: Kimppa K., Whitehouse D., Kuusela T. & Phahlamohlaka J. (eds.) *ICT and Society. 11th IFIP TC 9 International Conference on Human Choice and Computers, HCC11 2014, July 30 – August 1, 2014, Turku, Finland*. Heidelberg, Springer. pp. 78-91.
  Available from: https://doi.org/10.1007/978-3-662-44208-1_8

- Park, A. (2011) Beware paradigm creep and buzzword mutation. *Forestry Chronicle*. 87 (3), 337-344.

- PERSONA project (2019) *D1.2: Use-cases and user/technical requirements*.
  Available from: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5cdc86d68&appId=PPGMS [Accessed 30 March 2021].

- Reymen, I. M. M. J., Whyte, J. K., & Dorst, C. H. (2005) Users, designers and dilemmas of expertise. In: *Proceedings Include 2005, International conference on inclusive design, Royal college of Art, April 5–8, 2005, London, UK*. pp. 1-, Royal college of Art.
  Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.297&rep=rep1&type=pdf [Accessed 30 March 2021].

- Saariluoma, P. (2005) Explanatory frameworks for interaction design. In: Pirhonen A., Saariluoma P., Isomäki H. & Roast C. (eds.) *Future Interaction Design*. London, Springer. pp. 67-83.
  Available from: https://doi.org/10.1007/1-84628-089-3_5

- Saariluoma, P., Cañas, J. J., & Leikas, J. (2016) *Designing for life: A human perspective on technology development*. London, Palgrave Macmillan.

- SMILE project (2019) *D2.5. User and business requirements definitions including foresight application scenarios: Final Report*.
  Available from: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c8e797b5&appId=PPGMS [Accessed 30 March 2021].

- Taitto, P. & Hyttinen, K. (2018) EU's integrated approach to respond crisis and conflicts. In: Kīsnica, K. (ed.) *Organization and individual security*. Riga, Latvia, Turiba University, pp. 275-291.

- Uday, P. & Marais, K. (2015) Designing Resilient Systems-of-Systems: A Survey of Metrics, Methods, and Challenges. *Systems Engineering*. 18 (5), 491-510.
  Available from: https://doi.org/10.1002/sys.21325

- Wallach, D & Scholz, S.C. (2012) User-Centered Design: Why and how to put users first in software development. In: Maedche A., Botzenhardt A. & Neer L. (eds.) *Software for people. Management for professionals*. Heidelberg, Springer. pp. 11-38.
  Available from: https://doi.org/10.1007/978-3-642-31371-4_2