Chapter

Validation Strategy as a Part of the European Gas Network Protection

David Rehak, Martin Hromada, Ilias Gkotsis, Anna Gazi, Evita Agrafioti, Anastasia Chalkidou, Karolina Jurkiewicz, Fabio Bolletta and Clemente Fuggini

Abstract

The European gas network currently includes approximately 200,000 km high pressure transmission and distribution pipelines. The needs and requirements of this network are focused on risk-based security asset management, impacts and cascading effects of cyber-physical attacks on interdependent and interconnected European Gas grids. The European SecureGas project tackles these issues by implementing, updating, and incrementally improving extended components, which are contextualized, customized, deployed, demonstrated and validated in three business cases, according to scenarios defined by the end-users. Just validation is considered to be a key end activity, the essence of which is the evaluation of the proposed solution to determine whether it satisfies specified requirements. Therefore, the chapter deals with the validation strategy that can be implemented for the verification of these objectives and evaluation of technological based solutions which aim to strengthen the resilience of the European gas network.

Keywords: critical infrastructure, European gas network, validation, key performance indicators, resilience, protection

1. Introduction

The European gas network is an important and irreplaceable subsector of European Critical Infrastructure (ECI) [1]. The functioning of this network is constantly affected by threats with a direct but also cascading or synergistic effect [2]. These threats can be of various natures, e.g. meteorological, geological, process-technological, cascading, personnel, cyber or physical [3]. The impact of these threats can result in serious disruption or even failure of the regional parts of the gas network. For this reason, it is necessary to continuously improve the protection system of the European Gas Network, in particular through risk analysis and the consequent strengthening of the resilience through the identification and elimination of the identified weaknesses.

One of the main measures and means to achieve the enhancement of resilience, is through technological solutions, which should address the operational and technical needs of the infrastructure and requirements of the end user, i.e. infrastructure operator [4]. The chapter therefore deals with the validation strategy [5] that can be implemented for the verification of these objectives and the evaluation of technological based solutions which aim to strengthen the resilience of the

European gas network. The main objective of the proposed validation plan, as part of an overall evaluation process, is to study the acceptance of a designed security system aiming to promote resilience [6] of gas critical infrastructures (at strategic, tactical and operational level). For this purpose, it is necessary to collect qualitative information concerning some key criteria of the system which define its performance in the operations. The primary focus of the validation strategy is to assess the functionality and effectiveness of the proposed system. However, the intuitiveness of the individual components as well as the overall exploitation and operationalization potential of the developed solution, should also be evaluated.

The aforementioned validation plan has been developed and verified through continuous interaction with critical infrastructure (CI) operators within the SecureGas project [7]. The project aims to improve the resilience capabilities of the gas CI. The methodology uses a gas CI-contextualized Panarchy loop [8] reflecting a disaster life-cycle management process. The objective is to reduce foreseen risk, optimize the monetary investment, and reduce uncertainties. Providing the CI operators with a detailed validation methodological procedure to assess the added value of security solutions added to their infrastructure is of high value. Within the context of the SecureGas validation and evaluation, the following aspects that are addressed include: performance versus expectation, ease-of-use, understandability, reliability of operations, completeness and reliability of output, functionality, man–machine interface and efficiency. The criteria for validation, i.e. Key Performance Indicators (KPIs) [9], can be clustered into two categories: (1) general criteria that apply to the whole SecureGas system, and (2) specific criteria that apply to individual components of the system.

Such validation plan is fully transferable to other CI operators both of Gas and other sectors (e.g. power, telecommunication). With a slight adjustment of the identified KPIs, it can provide a valuable information on the applicability and usefulness of a security solution for risk mitigation, prevention and response purposes within a CI.

2. Validation, verification and evaluation

In order to understand the activities to be implemented from the validation point of view, definitions of the basic concepts used and are further analyzed below, presenting also several methodological approaches. Therefore, this section provides both a background analysis for validation-verification-evaluation processes and an adequate methodology.

The validation process involves the collection and evaluation of data, from the process design stage through commercial production phase, which establishes scientific evidence that a process meets a determined requirements. Process validation involves a series of activities taking place over the process. Regulatory authorities like European Medicines Agency and Food and Drug Administration have published guidelines relating to process validation [10]. The purpose of process validation is to ensure that varied inputs lead to consistent and high quality outputs. Process validation is an ongoing process that must be frequently adapted as manufacturing feedback is gathered. End-to-end validation of production processes is essential in determining product quality because quality cannot always be determined by a finished-product inspection. Process validation can be broken down into three steps: (1) process design, (2) process qualification, and (3) continued process verification.

The Guide to the Project Management Body of Knowledge (PMBOK guide), a standard adopted by the Institute of Electrical and Electronic Engineers, defines validation and verification as follows [5]:

- Validation: The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance and suitability with external customers. Contrast with verification.

- Verification: The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process. Contrast with validation.

These terms generally apply broadly across industries and institutions. In addition, they may have very specific meanings and requirements for specific products, regulations, and industries. Some examples: Software [11], Food and drug, Health care [12], Greenhouse gas [13], Traffic and transport [14], Simulation models [15], ICT industry, Civil engineering [16], Economics, Accounting, Agriculture, Arms control.

In the context of the above, validation can generally be classified into five basic categories:

- Prospective validation comprises the missions conducted before new items are released to make sure the characteristics of the interests which are functioning properly and which meet safety standards [17]. Some examples could be legislative rules, guidelines or proposals [18–25].

- Retrospective validation is a process for items that are already in use in distribution or production. The validation is performed against the written specifications or predetermined expectations based upon their historical data/evidences that are documented/recorded. If any critical data is missing, then the work cannot be processed or can only be completed partially [10]. Retrospective validation is used for facilities, processes, and process controls in operation use that have not undergone a formally documented validation process. Validation of these facilities, processes, and process controls is possible by using historical data to provide the necessary documentary evidence that the process is doing what it is believed to do. Therefore, this type of validation is only acceptable for well-established processes and would be inappropriate where recent changes in the composition of product, operating processes, or equipment have occurred [26].

- Concurrent validation is used for establishing documented evidence that a facility and processes do what they purport to do, based on information generated during actual imputation of the process [26]. This approach involves monitoring of critical processing steps and end product testing of current production to show that the manufacturing process is in a state of control.

- Cross-validation is an approach by which the sets of scientific data generated using two or more methods are critically assessed [27].

- Re-validation is carried out for the item of interest that is dismissed, repaired, integrated/coupled, relocated, or after a specified time lapse. Examples of this category could be relicensing/renewing driver's license, recertifying an analytical balance that has been expired or relocated, and even revalidating professionals [28]. Re-validation may also be conducted when a change occurs during the courses of activities, such as scientific researches or phases of clinical trial transitions.

In contrast, evaluation is a systematic assessment of a subject's qualities, using criteria governed by a set of standards. Evaluation involves tests or studies conducted to investigate and determine the technical suitability of an equipment, material, product, process, or system for the intended objective. So evaluation can be formative that is taking place during the development of a concept or proposal, project or organization, with the intention of improving the value or effectiveness of the proposal, project, or organization. It can also be summative, drawing lessons from a completed action or project or an organization at a later point in time or circumstance. [29]

According to the way the evaluation is conducted we can distinguish the following types [30]:

- Internal evaluation, carried out by organizations, groups or stakeholders directly involved in the implementation of the project solution.

- External evaluation, carried out by specialists outside the development team, who are not employed within the organization responsible for the project under evaluation and who have no personal, financial or direct interest in the project.

Evaluation can be characterized as being either formative or summative. Broadly (and this is not a rule), formative evaluation looks at what leads to an intervention working (the process), whereas summative evaluation looks at the short-term to long-term outcomes of an intervention on the target group [31]:

- Formative evaluation takes place in the lead up to the project, as well as during the project, in order to improve the project design as it is being implemented (continual improvement). Formative evaluation often lends itself to qualitative methods of inquiry.

- Summative evaluation takes place during and following the project implementation, and is associated with more objective, quantitative methods.

Process evaluation is an inductive method of theory construction, whereby observation can lead to identifying strengths and weaknesses in program processes and recommending needed improvements [32]. For this purpose, qualitative methods are most often used, which are defined in the context of evaluation as research methods that emphasize depth of understanding, that attempt to tap the deeper meaning of human experience, and that intend to generate theoretically richer, observations which are not easily reduced to numbers [32]. The most used qualitative evaluation methods include [33]: content analysis, situational analysis, in-house surveys and interviewing.

Content analysis involves studying documents and communication artifacts, which might be texts of various formats, pictures, audio or video [34]. Quantitative content analysis highlights frequency counts and objective analysis of these coded frequencies [35]. Additionally, quantitative content analysis begins with a framed hypothesis with coding decided on before the analysis begins. These coding categories are strictly relevant to the researcher's hypothesis. Quantitative analysis also takes a deductive approach [36].

Situation analysis refers to a collection of methods that managers use to analyze an organization's internal and external environment to understand the organization's capabilities, customers, and business environment. The situation analysis consists of several methods of analysis: The 5Cs Analysis, SWOT analysis and Porter five forces analysis [37]. These analyses help understand the analytical processes by which managers understand themselves, their consumers, and the marketplaces in which they compete.

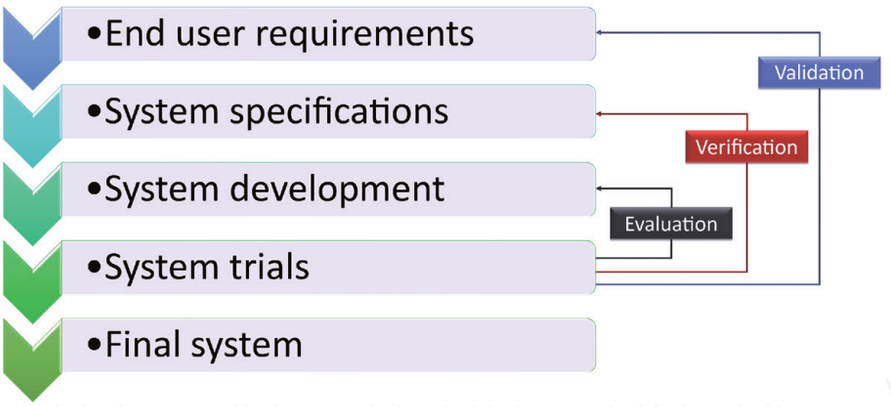

Figure 1.
Quality assurance framework.

SWOT analysis is a strategic planning technique used to help a person or organization identify strengths, weaknesses, opportunities, and threats related to business competition or project planning [38]. It is designed for use in the preliminary stages of decision-making processes and can be used as a tool for evaluation of the strategic position of an organization. It is intended to specify the objectives of the project and identify the internal and external factors that are favorable and unfavorable to achieving those objectives. Users of a SWOT analysis often ask and answer questions to generate meaningful information for each category to make the tool useful and identify their competitive advantage.

An interview is essentially a structured conversation where one participant asks questions, and the other provides answers. Interviews can range from Unstructured interview or free-wheeling and open-ended conversations in which there is no predetermined plan with prearranged questions [39], to highly structured conversations in which specific questions occur in a specified order [40].

Other commonly used tools and techniques for evaluation purposes [41] can include especially observation, survey questionnaires, case studies, analytical models, expert panel's consultation, cost–benefit analysis (CBA), and multi-criteria analysis (MCA).

Normally validation, verification and evaluation are performed in a row allowing to estimate the completeness and consistency of the system and examining its technical appropriateness, as depicted in **Figure 1**.

To sum up, verification and validation heavily rely on earlier phases of the project. Verification is a rather technical process in which the main question is whether the system works properly. The validation process covers not only the demonstrations but also earlier meetings and discussions in which the requirements are refined. As already mentioned, verification of developed tool/solution is the process of determining that the system is built according to its specifications. Validation is the process of determining that the system actually fulfills the purpose for which it was intended. Evaluation reflects the value and the acceptance of the system by the end users and its performance.

3. Concept of creating a validation plan

Following the analysis and presentation of validation, verification and evaluation processes, in this section, a holistic (including all those three processes) validation plan, will be analyzed. In principal, an effective validation and evaluation plan, needs to seek, as clear as possible, answers to the following issues:

1. What has to be evaluated?

2. Who is interested in the validation/evaluation?

3. What critical issues have to be tackled?

4. What has to be measured?

5. How validation/evaluation has to be performed?

6. Who is involved in the evaluation?

7. How results will be reported?

All these questions have been taken under consideration and are answered and described in detail as part of the SecureGas validation-evaluation methodological approach. In this four-step methodology (**Figure 2**), a set of business cases (BCs) is used to support the validation, verification and evaluation of SecureGas solution. Three BCs, addressing relevant issues for the gas sector (production, transport and distribution phase of the gas lifecycle, including different infrastructures for each phase) have been identified to ensure the delivery of solutions and services to the end-users. During the BCs implementation, tailor-made scenarios for the CIs will be used for demonstrations on actual sites. The technical components involved will be assessed quantitively (by measuring foreseen KPIs) and qualitatively (by using a set of questionnaires and interviews to the participants in the demonstrations).

3.1 Set the context

This kick-off step entails all the discussions and reviews with relevant stakeholders for the exact identification of the gaps and the existing capabilities. This step also sets the scope and the objectives of each BC for the SecureGas solution to provide differentiation from current practices and added value to the operational environment of a gas CI.

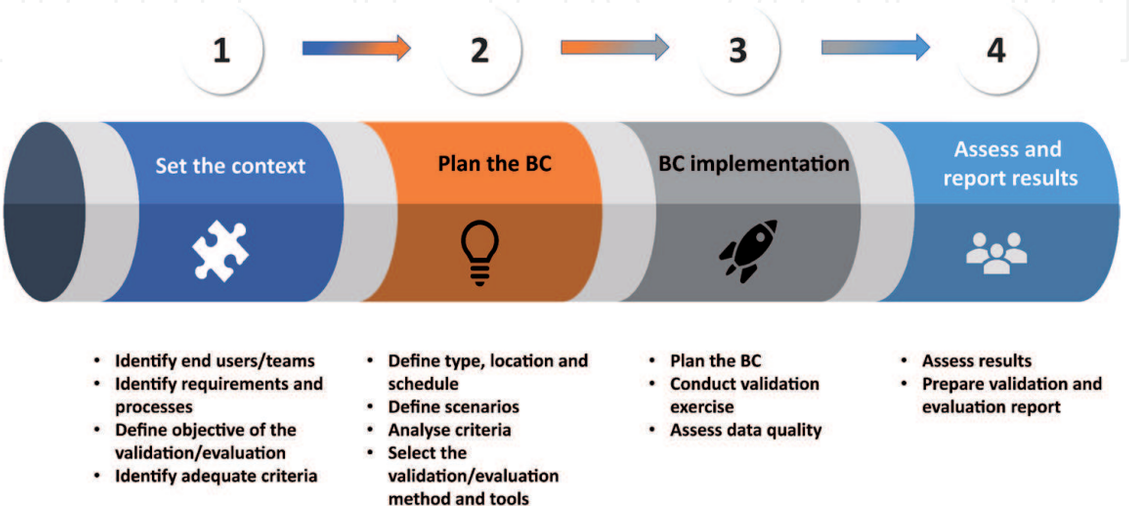

Figure 2.
SecureGas validation-evaluation methodology.

3.1.1 Identify end users/teams

Within SecureGas framework, the end-user team consists of the gas CI operators participating in the project (DEPA, EDAA, AMBER, ENI). Further to them, the SecureGas technical component providers are actively engaged and directly involved in all phases of the validation plan. External stakeholders have been identified and will be involved only in the BC implementation phase. They will participate and provide feedback for evaluation purposes. The stakeholders/actors participating in the pilot activities may vary among the different BCs however they belong to one of the following groups:

1. CI operators, managers and administrators, security liaison officers (also from interconnected, interdependent or similar CIs);

2. Emergency response authorities (police, fire brigade, civil protection, etc.);

3. National Authorities (CI regulatory authorities, ministries, etc.);

4. Security service providers;

5. Secondary/other security professionals and practitioners (e.g. policy makers, other EU research projects, etc.).

3.1.2 Identify requirements and processes

The SecureGas validation and evaluation process is an essential part of the project's development cycle. The development cycle is user-oriented, which means it relies on the perception, needs and responses by end users. Based on this development cycle, in SecureGas phase 1: "construct/develop", user requirements and specifications are identified leading to conceptual model (CM), concept of operations (ConOps) and high level reference architecture (HLRA). The CM, ConOps and HRLA will be implemented and demonstrated in phase 2: "demonstrate" and finally validated in phase 3: "validate & exploit".

Initial and crucial substeps to achieve an efficient planning and implementation of the BC are to:

1. Identify CI assets, threats, vulnerabilities, requirements, procedures, etc., in order to prepare the scenario including CI's specific security issues and addressing end users' actual needs.

2. Identify legacy systems and existing infrastructures, integration-data sharing, possible limitations, etc., and collaborate with the technical team to develop a SecureGas solution tuned to the project's BCs.

For the execution of these substeps, some may choose from a set of existing tools and frameworks, e.g. risk and vulnerability assessment and penetration testing (see Section 4).

3.1.3 Define the objective of the validation-evaluation process

The main objectives of the evaluation process will be to study the acceptance of the SecureGas system (at the strategic, tactical and operational levels), assess the performance of its components and the operational potential of the developed solution.

The beneficiaries of the validation and evaluation process are both technical component providers and CI operators. The technical providers will receive valuable feedback on technical development, components adaptation and implementation, system integration and cooperation with legacy systems, etc.. The CI operators will receive the performance assessment analysis of SecureGas solution, the extracted lessons, recommendations and conclusions, and all knowledge that can be transferred to their operations.

3.1.4 Identify adequate criteria

The criteria for validation can be clustered into two categories, further analyzed in Section 4:

- General criteria, that apply to the whole SecureGas system (cross-KPIs) and
- Specific criteria that apply to individual components of the system.

As such, the validation process will generate feedback during the pilot demonstrations on the following dimensions: functional, interface, security, operational, design, and implementation.

When it comes to the specific criteria, the SecureGas partners will make use of the lists of user (organizational, operational and regulatory) and technical (and standards-related) requirements defined, in order to determine whether the SecureGas system offers what it was designed to. As far as verification is concerned, the system specifications developed by technical partners will play the same role as user requirements in validation (see **Figure 1**). The evaluation process will also assess whether the SecureGas system complies with the technical requirements developed in Phase 1 of the project.

3.2 Plan the business case

This second part consists of a number of substeps that will lead in the realization of the BC implementation.

3.2.1 Type, location and schedule

In each SecureGas BC, an operational based demonstration will take place in the field (for the production, transport and distribution phases of gas lifecycle), aiming to simulate scenarios as realistically as possible in a controlled environment. This method of BC implementation will offer the advantage of real-time decisions and actions by the end-users and other participating actors, generating responses and leading to several consequences depending on the participants' actions and system performance. On top of that, regarding the strategic level of Gas lifecycle, a discussion-based approach will be followed, through the organization of a workshop/tabletop exercise, during which key personnel of the CI will have the chance to discuss scenarios that involve strategic threats and will assess policies, procedures, standard operating procedures and potential mitigation measures.

The locations may be related to the assets involved, the objectives and requirements of the validation, etc. Within SecureGas, the CI operators' sites in Greece, Lithuania and Italy have been selected and included in the scenarios based on the type of their installations.

Within the SecureGas project, project partners will customize, integrate and deploy the provided technical components into each BC. The deployment of the

extended and integrated components in the BC will be tested through piloting activities for a period lasting almost one year period, with the last months focusing on the evaluations leading to an overall report based on the data and information collected.

3.2.2 Define scenarios

BCs are based on scenarios that correspond to a sequence of facts occurring in a specific space–time framework. Scenarios should be structured in a logical, readily accessible way to the pilot actors. Within SecureGas BCs, scenarios consist of events designed to guide the actors towards achieving the BC objectives. Six specific methodological substeps have been specified to define the scenarios:

Substep 1: Identification of normative, institutional and legislation frameworks.
Substep 2: Identification of end-user's infrastructures, assets and pilot site attributes.
Substep 3: Involved stakeholders and pilot actors.
Substep 4: Considered threats and risk.
Substep 5: Unfolding the scenario.
Substep 6: Deployment of the SecureGas solution.

3.2.3 Analyze criteria

The criteria used for the validation/evaluation of the SecureGas system and each component, consist of cross KPIs and specific KPIs (all linked with the end user requirements and technical specifications). In Section 4.1, these criteria will be discussed in detail.

3.2.4 Select validation/evaluation method and tools

In the framework of the validation plan, the methods and tools for the evaluation needs have been selected. Thus, the following substeps are executed for each BC:

1. Define what has to be measured for based on applicable KPIs.

2. Define how, through discussion-based workshop/tabletop exercise for the strategic level, and operations-based simulations/field pilots for the tactical/operational level.

3. Define who are involved in the frame of the evaluation, sorted into three main groups as follows:

    - CI operators, security liaison officers, administrators and managers who can provide input based on an operational, policy and technical point of view, and evaluate the overall performance based on their experience.

    - First responders, who can provide input regarding the information sharing and community awareness during an incident.

    - Security practitioners and stakeholders, who, depending on their expertise, will provide information concerning the potential exploitation and use of the SecureGas solution. They may provide feedback on their willingness to use or adopt the system, other technical/operational comments, etc.

In order to achieve an effective evaluation outcome, the selection of the stakeholders, must be based on some requirements, such as the relevance to the scenario, adequate qualification, objectivity, previous experience.

4. Define the tools to be used to collect the results and feedback comprising:

   - KPIs and respective traceability matrices, for validation purposes, and
   - survey questionnaires, focus groups, interviews and brainstorming, for evaluation purposes.

5. Define how the results will be reported.

The results will be presented in suitable style and form, according to the reporting target audience and the selected tool. All reporting activities will be planned accordingly, paying attention to the most suitable communication means for the specific audience, in terms of content presentation, type of language, level of details and so on. For example, the elaboration of the questionnaires, the feedback from the interviews of the focus groups and the conclusions of the debriefing sessions (hot and cold washes) of BCs will be documented based on standardized feedback sheets which will be analyzed to improve the overall specification and development processes and their outcomes.

3.3 Business case implementation

The third part that will be followed in the validation plan, is that of that of the BC pilots execution, including both preparatory meetings and the actual field testing consisting of the following three substeps.

3.3.1 Plan the business case

1. End-users (internal and external) are identified specifically for each BC.
2. Identify the place and date and estimate the budget-plan logistics.
3. Send invitations, share information for the pilot with involved stakeholders.
4. Before the pilot, organize a training course, for the participants to have the opportunity to familiarize with the SecureGas solution.
5. The scenario (depending on the area of application) is presented to the end-users and its details are discussed.
6. All necessary adaptations, installations, integrations have been achieved and the system is ready to be used, demonstrated and evaluated.

3.3.2 Conduct validation exercise

Following the specific BC scenario storyline, the involved actors are guided and supported by the capabilities of the SecureGas system in order to respond to a security incident.

3.3.3 Assess data quality

Following the BCs pilots' implementation, the participants are asked to use the validation/evaluation tool/method (e.g. fill a specifically designed questionnaire, see Section 4). In some cases, interviews are held.

The assessment of results and feedback gathered leads to a holistic evaluation outcome, respective lessons identified and recommendations for further analysis.

3.4 Assess results

This last step of the methodology contains the analysis of the gathered evaluation results as well as an assessment of the SecureGas solution. The results of this step will be presented in the overall SecureGas evaluation and lessons identified report.

3.4.1 Assess results

The results assessment aims to collect valuable feedback from the end-users interactions during the pilots (via questionnaires, described in detail in Section 4.4), expressed opinions and comments through focus groups and end-session interviews. The purpose of this substep is to indicate among others whether the SecureGas solution is performing well, provides useful information, is easy to understand, reliable, ergonomic, efficient, etc.

3.4.2 Prepare validation and evaluation report

The final step in each BC pilot demonstration will summarize and present all the activities realized and the responses by involved actors' (both consortium partners and external experts). Based on these outcomes, an overall performance evaluation of the SecureGas solution will be reported, lessons, recommendations and conclusions will be extracted, and content for knowledge transfer will be structured.

4. Validation and evaluation tools

Within the SecureGas framework and specifically in the third phase of the project, that of validation and exploitation, several tools will be used in order to support the efficient implementation of the validation plan described in Section 3 above. These tools consists of: (a) an initial assessment tool, that will be used as a decision support tool to carry out a self-assessment to identify the level of intrusiveness and level of maturity of the CI, (b) the penetration testing tool/methodology for identifying vulnerabilities and assessing performance, (c) the KPIs that will be used as benchmarks to assess project's efficiency in reaching its key objectives and to evaluate the quality of the proposed technical solution, and finally (d) questionnaires and interviews as two main instruments for evaluation purposes.

4.1 Initial assessments

In the first step of the validation plan, the context is set as described in subSection 3.1. The validation plan follows the same approach as a pre-attack phase gathering as much information as possible on the target systems and planning the activities performed during the tests. Assessment frameworks such as [42, 43] can be used to identify the level of intrusiveness and level of maturity.

The substeps that are performed comprise:

1. Identify and prioritize assets: A list of identified assets indicating the importance of each one should be identified (e.g. software, hardware, data, interfaces, security governance, security controls and components, etc.).

2. Identify threats: A threat is anything that could exploit a vulnerability to breach security and cause harm to a CI. General threat categories are: physical adversarial threats and acts of terrorism, political/geopolitical/social threats, natural hazards, technological and accidental hazards, indirect threats and cyber threats.

3. Identify Vulnerabilities: Identify a list of known vulnerabilities of all the asset list and analyze the impact on the system/infrastructure if these are not correctly treated and mitigated The impact on the system shall be treated in terms of e.g. economy, reputation, and security for people

4. Analyze measures: Analyze the measures that are either in place or in the planning stage to minimize or eliminate the probability that a threat will exploit a vulnerability in the system

5. Determine the likelihood of an incident: The possibility of an incident to be an exploited vulnerability should be quantified, based on historical/statistical data, user experience and knowledge or any other sources available (e.g. studies, estimations/information that authorities are producing, etc.).

6. Assess the impact a threat could have, including factors such as the mission, the criticality and the sensitivity of the system and its data

7. Prioritize the security risk: For each threat/vulnerability pair, determine the level of risk for the system/infrastructure, based on the likelihood and the impact of the threat, and the adequacy of the existing or planned system/infrastructure security controls for eliminating or reducing the risk

8. Recommend Controls: Using the risk level from the previous step, determine the actions that the senior management of the CI and other personnel that hold key positions, must take to mitigate the risk to an accepted residual risk level.

9. Document the results to support management in making appropriate decisions on budget, policies, procedures, and so on.

4.2 Penetration testing

Following the above assessment, another process that can be used as a tool for identifying vulnerabilities and assessing performance is Penetration Testing (PT). PT is a security testing process in which experts execute real but yet controlled attacks on systems and services to identify methods for circumventing the security features of an application, system, or network [44].

PT methodologies divide the process into four generic phases:

1. A planning phase, focuses on gathering available information on the target systems, as well as on potential methods of attacks, management approval and setting the groundwork for setting up attack strategies and attack scenarios.;

2. A discovery phase, which is broken down into two parts: information gathering and scanning, and vulnerability analysis;

3. An attack Phase, where the tester put in place the knowledge acquired in the previous phase. This phase contains the following substeps: (a) Gaining access, (b) escalating privileges, (c) System browsing, and (d) Install additional tools;

4. A reporting phase, where experts evaluate findings and propose corrective actions.

4.3 Key performance indicators

KPIs typically enable the realization of technical systems towards tangible goals while serving as a benchmark for internal quality assurance. Indeed, KPIs are deemed as a measurable way to assess project's efficiency in reaching its key objectives and to evaluate the quality of the proposed technical solution(s). Through well-defined KPIs, the main areas to be tested, measured and validated during the piloting activities are established.

The SecureGas KPIs were defined in the early stage of the project so that they guide its targeted implementation. Preliminary activities, regarding user and system requirements identification as well as the CONOPS and HLRA definition, have already been completed providing valuable input to the KPIs definition task.

For the purposes of the SecureGas project, the KPIs were classified along two main indicator types:

a. SecureGas component KPIs, which reflect the key characteristics and functionalities offered by each SecureGas component and are applied for their performance evaluation;

b. SecureGas Cross-KPIs, which reflect the key functionalities and the expected quality of the entire SecureGas solution.

Both the SecureGas component KPIs and the SecureGas Cross-KPIs establish the validation criteria to be measured during SecureGas pilot demonstrations. Although both KPI categories are equally important for the evaluation of objectives' fulfillment, this section emphasizes on the KPIs defined for the integrated SecureGas system (i.e. SecureGas Cross-KPIs).

The methodology adopted for the definition of the KPIs was built on a bottom-up rationale. The SecureGas component KPIs (low level KPIs) were initially defined. Then, drawing on that information, the SecureGas Cross-KPIs (high level KPIs) were derived. The procedural pathway followed for the identification of KPIs is depicted in **Figure 3**.

Considering that KPIs depend on the end-users and stakeholders interested in the SecureGas system, the first step of the adopted methodology regarded their active engagement in the KPIs definition activities. This initiative had already started taking place through the definition of the user requirements (i.e. end-users needs and expectations from an integrated security system (such as the SecureGas system), as well as through dedicated stakeholders' workshops organized for the user requirements validation. The user requirements together with their external validation results shed light to those characteristics of the system that are deemed important by the end-users. In addition, information on the KPIs already applied by the end-users to assess the performance of their gas network daily operations allowed consortium partners to draft broad areas in which evaluations are

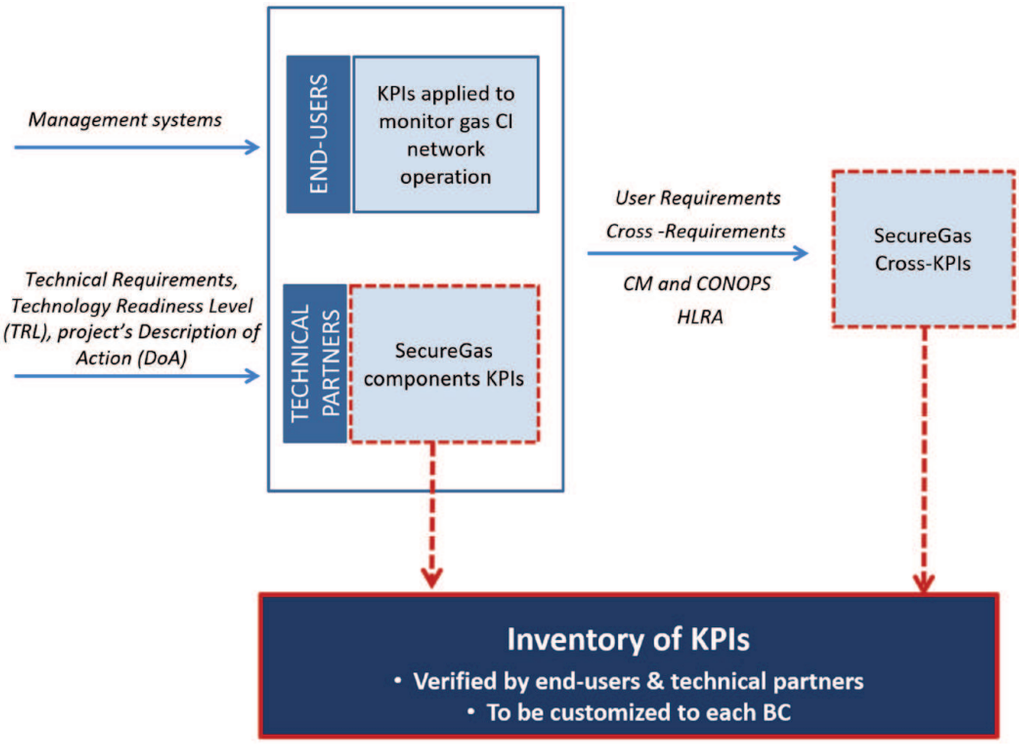

Figure 3.
KPIs definition pathway.

performed. This information also enabled the consortium to examine how the SecureGas solution could contribute and add value to the resilience of end-users' infrastructure.

In parallel, drawing on the already defined technical requirements of the SecureGas components, consortium technical partners defined the key capabilities, characteristics and functionalities offered by every technical subsystem. The so-called SecureGas component KPIs enable components' development and implementation.

The next step regarded the definition of the SecureGas Cross-KPIs which reflect the most important features and characteristics offered by the entire (i.e. all subsystems integrated into one system) SecureGas solution. The end-users KPIs, the SecureGas component KPIs and the already defined SecureGas system specifications (Cross-Requirements), provided the baseline for the extraction of a list of eleven SecureGas Cross-KPIs (**Table 1**) that are key to performance success.

As presented in **Table 1**, the SecureGas Cross-KPIs were classified into specific Fields that outline the general domain categories where the impacts are going to exert their effect. Those Fields are as follows:

- Reliability, i.e. the capability of the system to function in a correct manner within the given timeframe. This includes high accuracy of alert localization, avoidance of any delays in data provision, and a low rate of false alerts or errors.

- Autonomy, i.e. the level of independence of the system. An autonomous system is capable to operate (detect and process incidents) without human supervision (human in the loop only when deemed necessary).

- Interoperability, i.e. the ability of the system to work with new products (i.e. sensors or sub-systems) without special configurations.

Field	Indicator	Description	Metric	Target value
Reliability	False alert rate	Percentage of false alerts (both positive and negative) raised by the SecureGas system.	% (False alerts / Total alerts)	< 5%
	Cross correlation	Percentage of cross correlated alerts raised by the SecureGas system.	% (Cross correlated alerts / Total alerts)	> 50%
	Latency	Time elapsed between the moment an incident occurs and the moment the alert is displayed in the operational picture.	Time (sec)	< 10 sec
	Mean time to notify	Time needed for the operator to create an incident notification and send it to competent authorities/ stakeholders (escalation of incident).	Time (min)	< 3 min
Autonomy	Threat categories addressed	Number of different threats categories addressed by the SecureGas system (Threat categories: cyber, physical, cyber-physical, physical-cyber)	Number	4
	Automatic detection of threats	Number of different threat types automatically detected by the system. (Threat types: Intrusion detection, Third-Party Interference, Leak, Landslide hazard, Cyber)	Number	≥5
	Automatic decision-support	Percentage of alerts automatically linked to recommendations on crisis management and mitigation actions	% (Alerts with decision support / Total alerts)	≥ 80
Interoperability	Transparent integration of users' legacy systems	Number of users' legacy systems that can be easily and transparently integrated into the SecureGas system.	Number	≥1
Usability	Multilingual interface	Number of different languages in which the SecureGas user interface will be available	Number	4 (English, Italian, Greek, Lithuanian)
Resilience	Self-testing capabilities (system health check)	Percentage of components/ sensors that provide information to the operator - through dedicated alerts - about their status (not functioning and/or no communication)	%	90–95%
	Accuracy degradation percentage of a measurement value	The maximum decrease of accuracy (due to concept drift), before the model is retrained to adapt to background changes	%	20%

Table 1.
SecureGas cross-KPIs.

- Usability, i.e. is a set of attributes covering the effort needed for using a solution, and on the individual assessment of the use of the solution, by a stated or implied set of users.

- Resilience, i.e. is the ability of the SecureGas system to adapt from a disruption. This means that the system is able to identify potentially disruptive events and adapt to the evolving circumstances.

Each of the aforementioned Fields was linked to a set of Indicators, each one being assigned a Description, Metric and Target Value.

Following the main principles of the SecureGas project, the SecureGas Cross-KPIs aimed and achieved to addresses all the Risk and Resilience phases. Those phases reflect the activities that need to be conducted before, during and after disruptive events, as part of a comprehensive risk and resilience management procedure. The Risk and Resilience phases are as follows: Prepare, Detect, Prevent, Absorb, Respond, Recover, Learn and Adapt. The ultimate goal of developing Cross-KPIs for all those phases was to showcase how the core functionalities and performance indicators of the SecureGas system can add value to the enhancement of the resilience of gas critical infrastructure networks. **Figure 4** presents the Risk and Resilience phases that are affected by each SecureGas Cross-KPIs. Some of the Cross-KPIs are linked to one phase, some others to more, while the Cross-KPI "Multilingual Interface" is related to all the seven Risk and Resilience phases, since the enhancement of the usability parameters of a system has the potential to affect the entire security and resilience status of a CI network.

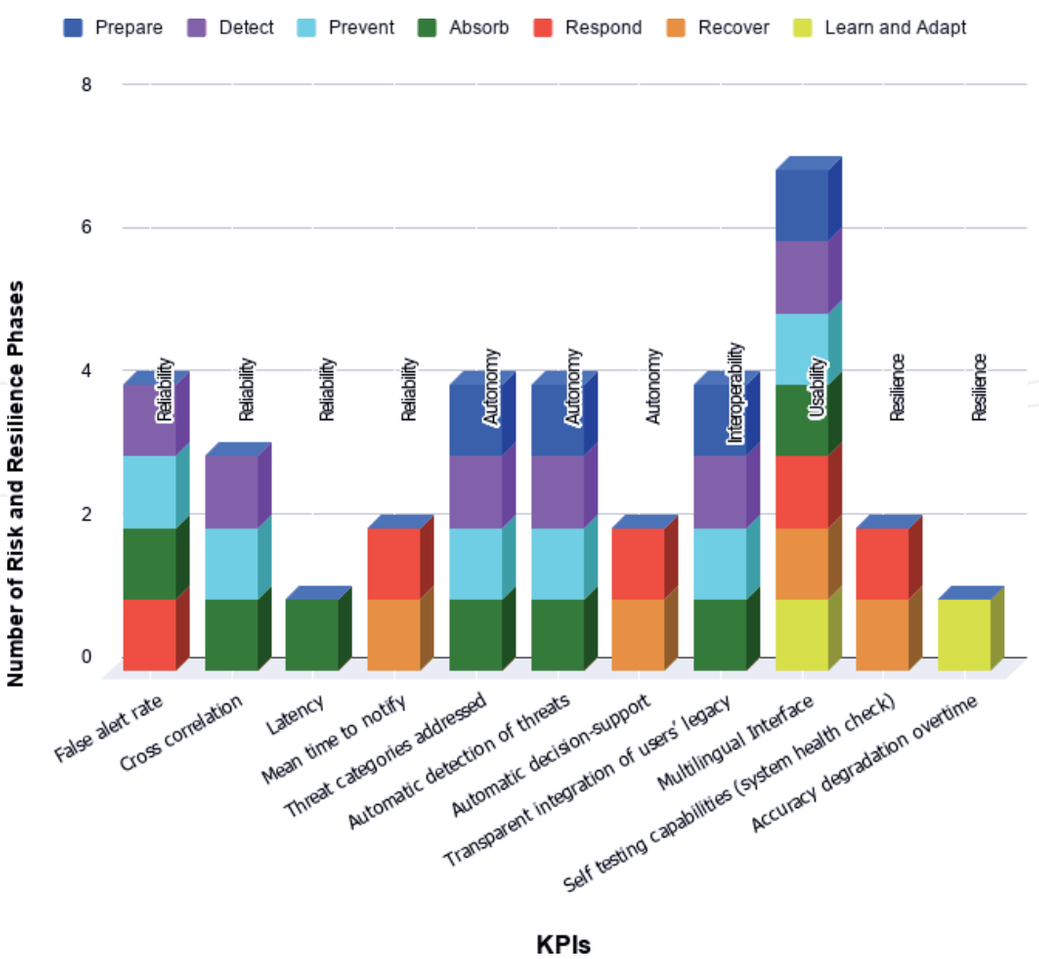

Figure 4.
Risk and resilience phases affected by each SecureGas cross KPI.

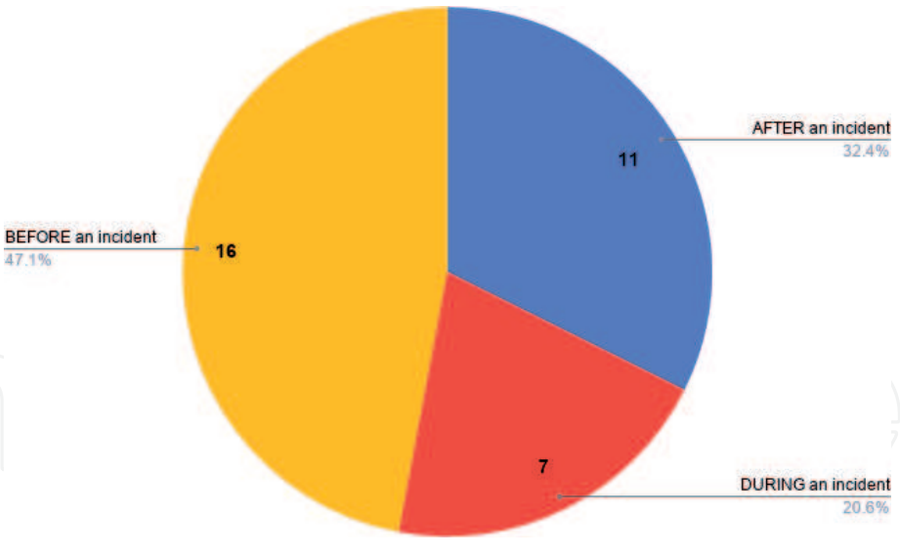

Figure 5.
KPIs distribution to the activities taking place before, during and after an incident.

Figure 5 shows the KPIs distribution to the activities taking place before, during and after incidents. In general, the SecureGas Cross-KPIs are mostly linked to the activities/phases taking place before the occurrence of an incident (prepare, detect, prevent) (approx. 47.1% of KPIs), although the SecureGas system do have performance parameters that are related to the post incident activities (response, recover, learn and adapt) (approx. 32.4%).

4.4 Questionnaires and interviews

Within the context of the evaluation of SecureGas components and solution, two main instruments will be used: questionnaires and interviews.

Regarding the first one, two types of questionnaires will be used for the evaluation purposes, one more generic that can be distributed to all participants (during testing, demonstrations, workshops) and one more specific, that would be filled by targeted participants within the audience, as further described below:

1. Questionnaire 1 (generic): This will be addressed to all participants of the BC demonstrations and is based on the System Usability Scale (SUS), developed by John Brooke in 1986 [45]. The questionnaire 1 provides a "quick and dirty" though reliable tool for measuring the usability of tested systems. SUS consists of a 10-item questionnaire with five response options for respondents; from strongly agree to strongly disagree. This allows to gather evaluation feedback concerning a wide variety of products, systems and services, including hardware, software, mobile devices, websites and applications. SUS has become an industry standard, with references in several articles and publications.

2. Questionnaire 2 (specific): The second questionnaire aims to extract end-users' assessed indicators on the basis of intuitiveness, usability, performance, etc. of the proposed solution. The end-users are going to fill-in this specific questionnaire after they have experienced the capabilities and the use of the system during the BC demonstration. This questionnaire is divided in seven main sections (i.e. general information, ease of installation, facilitation of user learning, data requirements, integrity, usability, usefulness), each one aimed at examining a different aspect of the end-users' view on the SecureGas components.

Regarding the second instrument for evaluation, indicative topics that may be used for discussion during the interviews comprise:

1. Experience and comments on the parallel processing, dataflow and cooperating applications within the SecureGas system.

2. Integration and interoperability of components, input/output and automatic/manual procedures for components.

3. Evaluation of SecureGas solution as a whole for the identification, detection, assessment and mitigation of threats and risk.

5. Conclusions

The validation framework is a key activity of every project, which broadly includes the validation of the proposed solution to determine whether it satisfies specified requirements, the verification of the system specifications, and the evaluation of the developed solution, all further analyzed as processes in Section 2. In the framework of the SecureGas project, the developed solution is a set of technological components and practical tools which aim to strengthen the resilience of the European gas network.

The envisaged validation framework (Section 3) mainly includes two types of assessment (Section 4): (a) Quantitative assessment, using a series of KPIs to validate components and the solution as a whole, (b) Qualitative assessment, based upon a dedicated questionnaire and interview, to get feedback from participants in the BCs implementation.

The methodological procedure, described in Section 3 of this chapter, is of no doubt necessary for any technological team providing a solution in order to identify potential gaps and updates needed. Furthermore, it is also valuable for end-users, in order to recognize the suitability of the proposed solution based on their requirements and specific security issues and appreciate the added value offered. Such validation framework is applicable, at least as a concept, to all projects offering technological solutions towards CI operators (or other type of end users) and can be adapted and tailor made to each case, leading to valuable feedback. On the other hand, the proposed methodology may need some adjustments, in order to cover the needs of an end-user that would like to assess and validate a process or a procedure that may have already in hand or is proposed (e.g. KPIs redefinition, questionnaires restructuring, etc.).

The next steps of this research contain the implementation of the BCs, based on this validation plan, and the documentation of the results of each BC, consolidating them into an overall validation and performance evaluation, which may lead to lessons identified, best practices and recommendations for the interested stakeholders.

Acknowledgements

The chapter was supported by the European Commission [Project SecureGas, GA No 833017] and the Ministry of the Interior of the Czech Republic [Project CIRFI 2019, GA No VI20192022151].

Conflict of interest

The authors declare no conflict of interest.

DOI: http://dx.doi.org/10.5772/intechopen.94644

Author details

David Rehak[1*], Martin Hromada[2], Ilias Gkotsis[3], Anna Gazi[3], Evita Agrafioti[4], Anastasia Chalkidou[4], Karolina Jurkiewicz[5], Fabio Bolletta[6] and Clemente Fuggini[6]

1 VSB – Technical University of Ostrava, Faculty of Safety Engineering, Ostrava, Czech Republic

2 Technology Platform Energy Security, Prague, Czech Republic

3 KEMEA - Center for Security Studies, Athens, Greece

4 GAP Analysis S.A., Athens, Greece

5 APRE – Agenzia per la Promozione della Ricerca Europea, Rome, Italy

6 Rina Consulting S.p.A., Genoa, Italy

*Address all correspondence to: david.rehak@vsb.cz

References

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Brussels: Council of the European Union.

[2] Rehak D, Senovsky P, Hromada M, Lovecek T, Novotny P. Cascading Impact Assessment in a Critical Infrastructure System. International Journal of Critical Infrastructure Protection. 2018:22:125-138. DOI: 10.1016/j.ijcip.2018.06.004

[3] Rehak D, Senovsky P, Hromada M, Lovecek T. Complex Approach to Assessing Resilience of Critical Infrastructure Elements. International Journal of Critical Infrastructure Protection. 2019:25:125-138. DOI: 10.1016/j.ijcip.2019.03.003

[4] Sullivant J. Strategies for Protecting National Critical Infrastructure Assets: A Focus on Problem-Solving. Hoboken, NJ: Wiley; 2007.

[5] IEEE Draft Guide: Adoption of the Project Management Institute (PMI) Standard: A Guide to the Project Management Body of Knowledge (PMBOK Guide)-2008 (4th edition). Piscataway, NJ: Institute of Electrical and Electronics Engineers; 2011.

[6] NIAC (National Infrastructure Advisory Council). Critical Infrastructure Resilience Final Report and Recommendations. Washington, DC: U.S. Department of Homeland Security; 2009.

[7] SecureGas project. Securing the European Gas Network [Internet]. 2020. Available from: https://www.securegas-project.eu/ [Accessed: 2020-09-18]

[8] Allen CR, Angeler DG, Garmestani AS, Gurdenson LH, Holling CS. Panarchy: Theory and Application. Ecosystems. 2014:17:578-589. DOI: 10.1007/s10021-013-9744-2

[9] Badawy M, El-Aziz AA, Idress AM, Hefny H, Hossam S. A Survey on Exploring Key Performance Indicators. Future Computing and Informatics Journal. 2016:1(1-2):47-52. DOI: 10.1016/j.fcij.2016.04.001

[10] Food and Drug Administration. Guidance for Industry Process Validation: General Principles and Practices [Internet]. 2011. Available from: https://www.fda.gov/files/drugs/published/Process-Validation--General-Principles-and-Practices.pdf [Accessed: 2020-08-04]

[11] Pham H. Software Reliability. Hoboken, NJ: John Wiley & Sons; 1999.

[12] Haggas R. Validation of electronic issue on the lth blood bank telepath system [Internet]. 2007. Available from: https://web.archive.org/web/20071012043133/http://www.transfusionguidelines.org.uk/docs/pdfs/oig_tools_qa_bb_e-issue_validation.pdf [Accessed: 2020-08-09]

[13] ISO 14064-1:2018. Greenhouse Gas Emissions and Removals Quantification and Reporting.

[14] Apeltauer T, Macur J, Holcner P, Radimsky M. Validation of microscopic traffic models based on gps precise measurement of vehicle dynamics. Promet – Traffic&Transportation. 2013:25(2):157-167. DOI: 10.7307/ptt.v25i2.1293

[15] Sargent RG. Verification and validation of simulation models. In: Jain S, Creasey RR, Himmelspach J, White KP, Fu MC, editors. Proceedings of the 2011 Winter Simulation Conference (WSC'11); December 2011; Phoenix, AZ: Winter Simulation Conference; 2011. p. 183-198.

[16] De Graaf RS, Vromen RM, Boes J. Applying systems engineering in the civil engineering industry: an analysis of systems engineering projects of a Dutch water board. Civil Engineering and Environmental Systems. 2017:34(2):144-161. DOI: 10.1080/10286608.2017.1362399

[17] Food and Drug Administration. Guideline on general principles of process validation [Internet]. 1987. Available from: https://web.archive.org/web/20090606085627/https://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm124720.htm [Accessed: 2020-08-16]

[18] Quinn J, McDermott D, Stiell I, Kohn M, Wells G. Prospective Validation of the San Francisco Syncope Rule to Predict Patients With Serious Outcomes. Annals of Emergency Medicine. 2006:47(5):448-454. DOI: 10.1016/j.annemergmed.2005.11.019. PMID 16631985

[19] Sangiovanni A, Manini M, Iavarone M, Fraquelli M, Forzenigo L, Romeo R, Ronchi G, Colombo M. Prospective validation of AASLD guidelines for the early diagnosis of epatocellular carcinoma in cirrhotic patients. Digestive and Liver Disease. 2007:40(5):A22-A23. DOI: 10.1016/j.dld.2007.12.064

[20] Germing U, Strupp C, Kuendgen A, Isa S, Knipp S, Hildebrandt B, Giagounidis A, Aul C, Gattermann N, Haas R. Prospective validation of the WHO proposals for the classification of myelodysplastic syndromes. Haematologica. 2006:91(12):1596-1604.

[21] Sciolla R, Melis F. Rapid Identification of High-Risk Transient Ischemic Attacks: Prospective Validation of the ABCD Score. American Heart Association. 2008:39(2):297-302. DOI: 10.1161/STROKEAHA.107.496612

[22] Pfisterer M, Bertel O, Bonetti PO, Brunner-La Rocca HP, Eberli FR, Erne P, Galatius S, Hornig B, Kiowski W, Pachinger O, Pedrazzini G, Rickli H, De Servi S, Kaiser Ch. Drug-eluting or bare-metal stents forlarge coronary vessel stenting? The BASKET-PROVE (PROspective Validation Examination) trial: Study protocol and design. American Heart Journal. 2008:115(4):609-614. DOI: 10.1016/j.ahj.2007.11.011

[23] Van Geest-Daalderop JHH, Hutten BA, Péquériaux NCV, Levi M, Sturk A. Improvement in the regulation of the vitamin K antagonist acenocoumarol after a standard initial dose regimen: prospective validation of a prescription model. Journal of Thrombosis and Thrombolysis. 2008:27(2):207-214. DOI: 10.1007/s11239-008-0203-4

[24] Ames D, Keogh AM, Adams J, Harrigan S, Allen N. Prospective validation of the EBAS-DEP – A short sensitive screening instrument for depression in the physically ill elderly. European Psychiatry. 1996:11(4):361s. DOI: 10.1016/0924-9338(96)89148-6

[25] Kidwell ChS, Starkman S, Eckstein M, Weems K, Saver JL. Identifying Stroke in the Field: Prospective Validation of the Los Angeles Prehospital Stroke Screen (LAPSS). American Heart Association. 2000:31(1):71-76. DOI: 10.1161/01.str.31.1.71

[26] Kneat Solutions. The Four Types of Process Validation [Internet]. 2017. Available from: http://blog.kneat.com/the-four-types-of-process-validation [Accessed: 2020-08-25]

[27] Food and Drug Administration. Bioanalytical Method Validation Guidance for Industry [Internet]. 2018. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/bioanalytical-method-validation-guidance-industry [Accessed: 2020-08-28]

[28] Merkur S, Mossialos E, Long M, McKee M. 2008. Physician revalidation in Europe. Clinical Medicine Journal. 2008:8(4):371-376. DOI: 10.7861/clinmedicine.8-4-371

[29] Scriven M. The methodology of evaluation. Lafayette, IN: Purdue University; 1966.

[30] Volkov BB, Baron ME. 2011. Issues in internal evaluation: Implications for practice, training, and research. New Directions for Evaluation. 2011:132:101-111. DOI: 10.1002/ev.399

[31] Owen JM, Rogers PJ. Program Evaluation: Forms and Approaches. Thousand Oaks, CA: Sage Publications; 1999.

[32] Rubin A, Babbie E. Research methods for social work. 4th ed. Belmont, CA: Wadworth/Thomas Learning; 2001.

[33] Bess G, King M, LeMaster PL. Process evaluation: How it works. American Indian and Alaska Native Mental Health Research. 2004:11(2):109-120.

[34] Bryman A. Business research methods. 3rd edit. Cambridge: Oxford University Press; 2011.

[35] Kracauer S. The Challenge of Qualitative Content Analysis. Public Opinion Quarterly. 1952:16(4):631-642. DOI: 10.1086/266427

[36] White MD, Marsh EE. Content Analysis: A Flexible Methodology. Library Trends. 2006:55(1):22-45. DOI: 10.1353/lib.2006.0053

[37] Steenburgh T, Avery J. Marketing Analysis Toolkit: Situation Analysis. Boston, MA: Harvard Business School; 2010.

[38] Humphrey A. SWOT Analysis for Management Consulting. Menlo Park, CA: SRI International; 2005.

[39] Yale JR. Frontier Thinking in Guidance. Chicago, IL: Science Research Associates; 1945.

[40] Kvale S, Brinkman S. Interviews: Learning the Craft of Qualitative Research Interviewing. 2nd ed. Thousand Oaks, CA: Sage; 2009.

[41] Morra-Imas LG, Rist RC. The road to results: designing and conducting effective development evaluations. Washington, DC: The World Bank; 2009.

[42] ISO/IEC 27001:2013. Information security management.

[43] ISO/IEC 27005:2018. Information security risk management.

[44] NIST 800-115:2008. Technical Guide to Information Security Testing and Assessment.

[45] UsabiliTEST. System Usability Scale (SUS) Plus [Internet]. 2020. Available from: https://www.usabilitest.com/system-usability-scale [Accessed: 2020-09-12]