# On the Assessment of Preservability: Method and Application

Diogo Proença, Gonçalo Antunes
IST/INESC-ID
Lisbon, Portugal
{diogo.proenca, goncalo.antunes}@ist.utl.pt

Tomasz Miksa
Secure Business Austria
Vienna, Austria
tmiksa@securityresearch.at

## ABSTRACT
This paper aims to establish engineering processes and methods for the assessment and deployment of digitally preservable systems by identifying a method for assessing the preservability capabilities of systems. The work done on this was based on the hypothesis that preservability consists of a set of systems capabilities that originates from a combination of system/software capabilities as defined in ISO 25010:2010. Based on that hypothesis, it was verified that such quality characteristics influence the preservability of systems. That influence is relative, since it depends on the specific scenario being addressed and on the concerns and requirements of the stakeholders of the system, as different qualities of a system might assume different degrees of importance along time. With those principles taken into account, this work developed an assessment method for assessing the preservability of systems that can be adapted to each scenario being analyzed. For demonstrating the application of the method, an example assessment was performed on a specific scenario, which resulted on the revelation that preservability of the system in focus on that particular case can be greatly improved.

## Categories and Subject Descriptors
H.1 [**Information Systems**]: Models and Principles; J.1 Administrative Data Processing Government; K.6.4 Management of computing and Information Systems.

## General Terms
Management, Documentation, Measurement, Verification.

## Keywords
Trust, Digital Preservation, Checklist Assessment.

## 1. INTRODUCTION
It can be said that the successful preservation of a business process depends on the capturing of context that is sufficient to be able to redeploy it in the future. However, different scenarios present different challenges considering the availability of that context for preservation. The technological context is such an example: some systems possess the necessary capabilities that make their preservation possible while others do not. In order to be able to easier distinguish between these systems, we introduce the concept of preservability.

We define **preservability** as the degree to which a system, product, or component can be archived for as long as necessary, ensuring its trustworthiness, and redeployed and re-executed according to the expectations, in a future environment, that might potentially be different from the original. This definition hints at the fact that the degree of preservability is always dependent on the requirements of the stakeholders, or in other words, it is dependent on the specific scenarios approached: different scenarios have different stakeholders with different needs concerning preservation. For instance, in some scenarios stakeholder‘s requirements might dictate that full functionality has to be preserved, while in other scenarios partial functionality might suffice.

Based on this definition, one can say that preservability seems to be a desired quality of systems, since it is usually not imposed by functional or business requirements. In fact, the hypothesis raised by this work claims that preservability is a set of system capabilities originating from a combination of system/software qualities. These system/software qualities assume different relevance among them depending on the scenario being assessed.

The subject of system/software qualities has decades of research. One of the most relevant references on this subject is the *ISO 25010:2010 – Systems and Software Engineering -- Systems and Software Quality Requirements and Evaluation (SQuaRE) – Systems and Software Quality Models10 [1]*. The standard defines a set of quality models that can be used in the identification of relevant system/software quality characteristics that can be further used to establish requirements, criteria for satisfaction and measures.

Based on the hypothesis raised, this work aims to define a method for the identification and assessment of relevant software qualities from the perspective of preservability. For that, the ISO qualities will be analyzed from the point of view of preservability. An assessment process based on *ISO 15504 - Information technology — Process assessment [2]* will be presented. Finally, a Civil Engineering Institution will be used to depict how the preservability of a real system could be assessed.

## 2. THE QUALITY CHARACTERISTICS OF SYSTEM’S PRESERVABILITY
The hypothesis raised by this paper is that preservability is attained via a set of system’s capabilities achieved by a combination of quality characteristics of systems. However, the assessment of preservability itself can be seen as a hard task since it involves present verification of something what can only be assured with full certainty in the future. Nonetheless, in order to be better prepared for being preserved and later redeployed in the future, systems should possess determined qualities.

The ISO 25010 defines quality characteristics for software systems which can be “further used to establish requirements, their criteria for satisfaction and the corresponding measures” [1]. It defines eight system/software product qualities: functional suitability, performance efficiency, compatibility, usability,

reliability, security, maintainability, and portability. In this section we relate these qualities to preservability, the definitions can be found in [1].

## 2.1 Functional Suitability

**Functional suitability** in terms of preservability, in some scenarios assumes particular importance, since the stakeholders might require that the system is fully functional when redeployed. The following aspects are considered sub-characteristics of functional suitability according to the ISO:

**Functional completeness:** In the perspective of preservability, this characteristic might assume particular importance in specific scenarios, where stakeholders require a fully functional redeployed system. In other scenarios, full functional completeness might not be so important, since the stakeholders might require only partial functionality to be redeployed.

**Functional correctness**: Concerning preservability, this characteristic might influence the decision to preserve. For instance, if a high degree of correctness is required by stakeholders, and if the system is not able to comply with it, then its preservation of the system might be ruled out.

**Functional appropriateness:** In terms of preservability, if the system does not possess this characteristic, then its stakeholders might not consider it particularly fit to be preserved.

## 2.2 Performance Efficiency

**Performance efficiency** in some scenarios this characteristic assumes particular importance, especially in scenarios where the stakeholders expect that the experience with the system remains unchanged. The following aspects are considered sub-characteristics of performance efficiency according to the ISO:

**Time behavior:** Concerning preservability, this characteristic becomes crucial if the stakeholders require the system's response and processing times to remain the same.

**Resource utilization:** Concerning preservability, the resource utilization might impact the choice to preserve or not a system, due to the high or low amounts of resources required or the expected availability of some types of resources in the future.

**Capacity:** In terms of preservability, this characteristic might assume importance in some scenarios since a system with greater capacity, might require more resources at the time of preservation, while a system with lower capacity might require less resources.

## 2.3 Compatibility

**Compatibility** is a very important aspect of digital preservation as after redeployment there is the need to assure that a system will perform as expected, despite having differences in the environment. Any incompatibility with other systems or any external dependency will endanger the preservability status of a system as the system might not perform as it was expected. The following aspects are considered sub-characteristics of compatibility according to the ISO:

**Co-existence**: In terms of preservability this attribute can be used in conjunction with the dependency capturing to check for possible dependencies that are critical for the correct execution of the system. It will also help to check if there are any incompatibilities between the system and other products, so that in the future we can use all this data to guarantee the correct execution of the system and eliminate the existence of any incompatibility.

**Interoperability**: In terms of preservability this attribute can be used to assess to what extent a certain system makes use of proprietary protocols, which can endanger the preservability of the system, due to licensing or third-party systems needed. This attribute can also be used to check with which other systems our system is communicating with and are essential for the correct execution of it, making it useful for dependencies capturing. Finally this attribute, can also be used as a measure of good communication channels between the system and other components which can enhance its preservability status.

## 2.4 Usability

**Usability** concerning preservability, usability might be important in determined scenarios with systems that involve heavy user interaction. The following aspects are considered sub-characteristics of usability according to the ISO:

**Appropriateness recognisability:** Depending on the scenario, this characteristic might impact the choice of doing preservation if, for instance, the scenario at hand requires or not the system to be appropriate for its users. This characteristic might also impact the success of adoption by future users after redeployment.

**Learnability**: Depending on the scenario at hand, it might impact the decision to preserve and might also impact the adoption by users after redeployment.

**Operability**: Depending on the scenario at hand, this characteristic might impact the success of adoption by future users after redeployment.

**User error protection:** Depending on the scenario at hand, this characteristic might impact the success of adoption by future users after redeployment.

**User interface aesthetics:** Depending on the scenario at hand, this characteristic might impact the success of adoption by future users after redeployment.

**Accessibility**: Depending on the scenario at hand, this characteristic might impact the success of adoption by future users after redeployment: if a system is currently difficult to use by a wide range of users, then it is probable that it will remain like that after redeployment.

## 2.5 Reliability

**Reliability** concerning preservability, might influence the decision to preserve a system. The following aspects are considered sub-characteristics of reliability according to the ISO:

**Maturity:** Concerning preservability, this characteristic might influence the decision to preserve a system, in the sense that a more mature system, will lead to less complications when preserving and redeploying.

**Availability:** Concerning preservability, this characteristic might influence the decision to preserve a system in certain scenarios, since a system which shows poor availability rates might not be considered for preservation.

**Fault tolerance**: Concerning preservability, this characteristic might influence the decision to preserve a system in certain scenarios, since a system which shows poor fault tolerance rates might not be considered for preservation.

**Recoverability**: This characteristic might be very important for preservability since it might facilitate the preservation and redeployment of the system.

## 2.6 Security

**Security** is a crucial aspect of digital preservation itself, since its impact might be positive or negative on the preservability of systems. Systems might manage sensitive data that should be considered when doing preservation. Additionally, systems might include mechanisms that can become troublesome to preservation. The following aspects are considered sub-characteristics of security according to the ISO:

**Confidentiality**: Confidentially might impact negatively the preservability of a system if, for instance, encryption mechanisms are being used in the system for securing accesses to the data, which would also involve preserving the encryption keys. Additionally, confidentiality might involve the use of external systems for managing the access to files.

**Integrity**: Integrity is considered a basic property of DP. In terms of preservability, it is desirable that a system has built-in integrity mechanisms, since that can be a guarantee that either the system or the data have not been changed in an unauthorized way prior to preservation. Integrity should then be ensured during the archive phase.

**Non-repudiation**: In terms of preservability, it is desirable that non-repudiation is ensured when preserving a system, since the historic of all actions or events happening before the system was preserved is important to ensure the provenance of the system and its data, ensuring the authenticity of the preserved objects. Provenance is necessary to validate the authenticity of preserved data, and includes the documented history of creation, ownership, accesses, and changes occurred over time.

**Accountability:** In terms of preservability, it is desirable that accountability be ensured when preserving a system, since the historic of all actions or events happening before the system was preserved, and its relation with different entities concerned with the system, is important to ensure the authenticity of the system and its data.

**Authenticity**: In terms of preservability, authenticity concerns the reliability of the objects in the sense that the control over their custody is enforced [1]. As such, it is a basic property of DP and often includes the existence of mechanisms for authentication and authorization as a way of enforcing it.

## 2.7 Maintainability

**Maintainability** is the ease of reconfiguration of the running system, product, or component by its maintainers and ability to cope with a changed environment. In case of digital preservation, the maintainers are the persons responsible for redeployment and the changed environment is the redeployment environment. When a system, product, or component is being redeployed it has to be fitted into the existing environment. The possibility to influence several settings and parameters of a system, product, or component increases the chance to redeploy it successfully. For example if a software which uses a database and external services have locations and addresses not hardcoded and therefore possible to modify, then the software has higher maintainability and higher preservability. However, in order to be able to benefit from maintainability a sufficient set of information describing the potential changes must be documented and preserved. Otherwise, high maintainability may decrease the preservability. The following aspects are considered sub-characteristics of maintainability according to the ISO:

**Modularity**: A System, product, or component with high modularity allows easy distinguishing between the modules. When any problems during redeployment occur, it is easier to deal with them within a module ("divide and conquer") rather than trace and identify their effects in the whole complex system, product, or component. Furthermore, different digital preservation actions may be suitable for different kinds of modules. Higher customization of digital preservation actions stemming from modularity should result in higher preservability.

**Reusability**: The higher reusability of a system, product, or component, the higher the likelihood that it is already a part of a knowledge base or a repository and therefore does not have to be the subject of digital preservation actions. Reusability of a system, product, or component may benefit from higher standardization. Furthermore, reusable systems, products, or components usually have broader community of users and thus more know-how and experience in preservation of these systems, products and components is available.

**Analyzability**: This is one of the critical requirements for preservability. The more information on execution of a system, product, or component is provided, the better the preservation actions can be adjusted. For example high analyzability facilitates identification of modules and their dependencies. Moreover, higher analyzability fosters the verification of system, product, or component redeployment. If some of modules cannot be redeployed, it may provide essential information to locate or reengineer substitute modules. Mechanisms like tracing, logging or provenance collection increase analyzability.

**Modifiability:** Modifiability is highly coupled with modularity and analyzability. It is very likely that, the more modular and analyzable the system, product, or component is, the easier it is to introduce and evaluate the modification. A need to modify the system, product, or component may occur when the preserved system, product, or component must be adjusted to the new redeployment environment, e.g. the database engine has to be substituted with a different one available on a different address.

**Testability**: While high analyzability allows passive collection of information, high testability allows active examination of a system, product, or component without affecting its state. It gives a possibility to design and run tests in the original environment. These tests can be executed in the redeployment environment and its results can be compared against original one. Moreover, testability allows verifying if any of introduced changes, like component substitution, are not affecting the system, product, or component in an undesired way.

## 2.8 Portability

**Portability** is one of the key aspects of digital preservation. In order to preserve a system we have to archive it and later redeploy it in a different environment. In this sense, a system with a high degree of portability will be highly desirable as it can be transferred without major incompatibilities of hardware, software or environment which will enhance its preservability status. The following aspects are considered sub-characteristics of portability according to the ISO:

**Adaptability:** In terms of preservability this attribute can be used to assess to what extent a system is prepared for different software, hardware or environments that might appear in the future. This is also a measure that can guarantee platform and hardware independence.

**Installability**: In terms of preservability this attribute can be important as a measure of easiness of installation of a certain system. An easy to install system is desirable as it ensures that there is fewer or no need for trained personnel to install the system, and reduces the total redeployment time. Moreover, if an installation procedure exists where is described how to install the system and/or automated installer exists it will enhance a system's preservability.

**Replaceability**: In terms of preservability this attribute can be used for alternatives assessment. In case other system or part of a system fails we can replace that system with an identified replacement system that will perform in the same way of the failing system. During redeployment, in case we can't redeploy the system due to missing dependencies, or any other reason, we can redeploy or use another system which was previously identified as replacement.

# 3. ASSESSMENT METHOD

This section contains the assessment process based on the guidance provided by ISO15504 [2], and serves as guidance on the nature of process required to assess preservability. The content of this process contains the minimum elements of a documented assessment process applicable for use in the context of assessing preservability.

Although this process includes only the activities, their description implicitly contains the other elements that may comprise a process: purpose, initial conditions, end condition, inputs, outputs, and roles and responsibilities.

The assessment process consists of the following activities: (1) Initiation, (2) Planning, (3) Briefing, (4) Data collection, (5) Data validation, (6) Analysis of the Preservability Assessment, and (7) Assessment reporting.

These activities are combined to form the assessment process for preservability depicted in Figure 1.

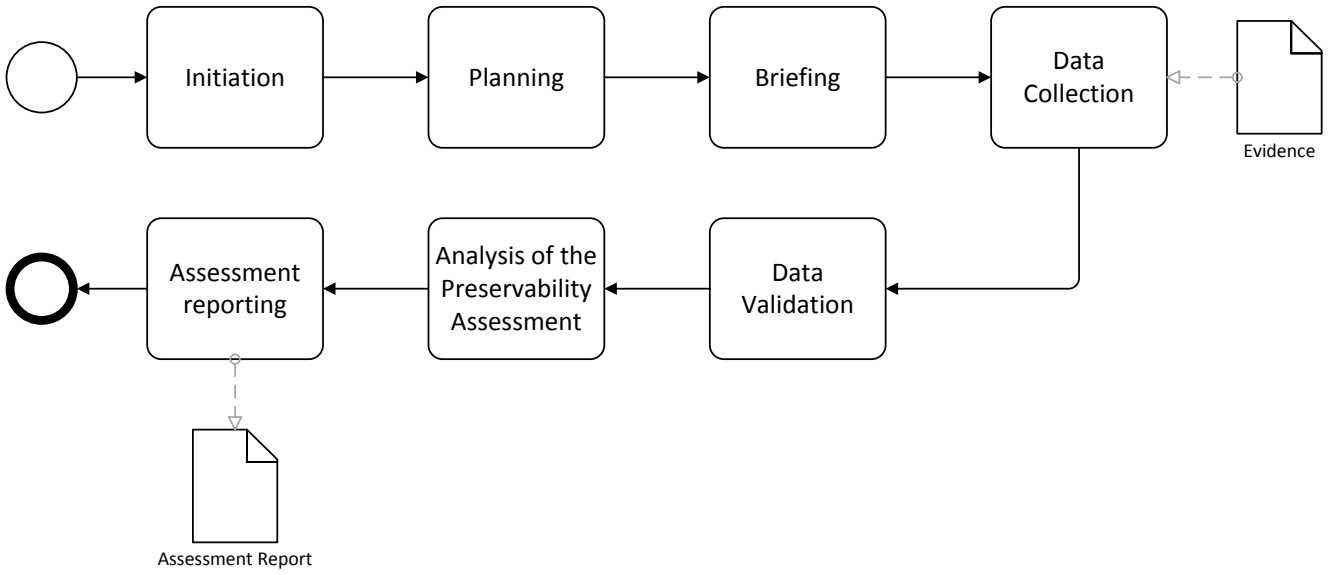


**Figure 1: Preservability Assessment Process**

## 3.1 Initiating the Assessment

### *3.1.1 Overview*

The assessment process begins by:

- identifying the stakeholders and defining the purpose of the assessment (why it is being carried out),
- defining what constraints, if any, apply to the assessment,
- identifying any additional information that needs to be gathered,
- choosing the assessment participants and the assessment team and defining the roles of team members,
- defining all assessment inputs and having them approved by the stakeholders.

### *3.1.2 Tasks*

**Identify the stakeholders** of the assessment.

**Select the Assessment Team Leader,** who will lead the assessment team and ensure that the persons nominated possess the necessary competency and skills.

**Define the assessment purpose** including alignment with business goals (where appropriate).

**Identify the need for and approve confidentiality agreements** (where necessary), especially if external consultants are being used.

**Select the Local Assessment Coordinator.** The Local Assessment Coordinator manages the assessment logistics and interfaces with the Organization.

**Submit Pre-Assessment Questionnaires to the Local Assessment Coordinator.** The Pre-Assessment Questionnaires help structure the on-site interviews by gathering information about the Organization and projects.

**Establish the assessment team and assign team roles.** Normally, the team should ideally consist of two assessors (depending on resource and cost). Assessment team members ensure a balanced set of skills necessary to perform the assessment. The assessment team leader should be a competent assessor.

**Define the context.** Identify factors in the Organization that affect the assessment process. These factors include, at a minimum:

- the size of the Organization,
- the application domain of the products or services of the Organization,
- the size, criticality and complexity of the products or services,
- the quality characteristics of the products,
- the preservability requirements in terms of quality characteristics of the Organization.

**Specify constraints** on the conduct of the assessment. The assessment constraints may include:

- availability of key resources,
- the maximum amount of time to be used for the assessment,
- specific Organizations to be excluded from the assessment,
- the minimum, maximum or specific sample size or coverage that is desired for the assessment,
- the ownership of the assessment outputs and any restrictions on their use,
- controls on information resulting from a confidentiality agreement.

**Define the goals of the assessment and create the assessment checklist.** The goals can be identified and modelled through a goal model (such as i* [4]) which can then be used to create the assessment checklist.

An example of the checklist created for a Civil Engineering Institution assessment regarding the Co-existence quality is shown in Table 1.

**Table 1: Co-Existence Assessment Checklist for a Civil Engineering Institution**

| No. | Compatibility | Evidence |
|---|---|---|
| **C1** | **Co-Existence** | |
| **C1.1** | **The system has a historic of compatibility errors which can be traced back to components and maintains an (in)compatibilities list.** *An historic of compatibility errors is very effective to determine the cause of an error as a first attempt, it can be useful to trace errors without much effort. Also, a list of compatibilities and incompatibilities can be used to set up the environment for the system. Example: Two versions of .NET framework installed in the same machine, an outdated driver.* | Logs; Compatibility Errors History Document; (In)compatibilities list; Evidence of continuous update of the (in)compatibilities list; Systems Logs; Document containing the history of errors and possible solutions; Existence of Hardware/Software compatibilities list; Evidence that the Hardware/Software compatibilities list is updated and useful. |
| **C1.2** | **There is a mechanism to check for dependencies of system's components and dependencies errors are analyzed by a support team.** *A mechanism to check for (external) components used by a system can help in further installations or exceptions handling, also the analysis of dependencies errors is essential to trace the errors and develop fixes. Example: the use of CUDF (ldd) in LINUX Environments, the use of the registry in Windows environments, dynamic library dependency (otool) in MAC OS.* | Evidence of previous dependency analysis; Evidence of periodic dependency analysis; Evidence of log analysis for co-existence errors; Logs. |

**Select the assessment participants** from within the Organization. The participants should adequately represent the quality characteristics in the assessment scope. As guidance we provide a

set of example organizational roles that can be found across organizations with different backgrounds and different sizes which is based on COBIT 5 [3]. Moreover, these organizational roles are mapped to the characteristics to be assessed in order to get the right people to the assessment. These are provided as guidance, not all organizations have these roles defined in their structure however the role descriptions can help an assessor to find the right people within the organization. The roles and their description are depicted in [5] and the mapping is presented in Table 2. In Table 2 the roles that were not used by any of the quality characteristics were omitted.

**Table 2: Mapping of the organizational roles and the preservability assessment characteristics**

| Id | Quality | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Privacy Officer |
|---|---|---|---|---|---|---|---|---|---|
| **C** | **Compatibility** | | **x** | **x** | **x** | **x** | **x** | | |
| C1 | Co-existence | | x | x | x | x | x | | |
| C2 | Interoperability | | x | x | x | x | x | | |
| **P** | **Portability** | | **x** | **x** | **x** | **x** | **x** | | |
| P1 | Adaptability | | x | x | | | x | | |
| P2 | Installability | | x | x | x | | x | | |
| P3 | Replaceability | | x | x | x | x | x | | |
| **M** | **Maintainability** | | **x** | **x** | | | **x** | | |
| M1 | Modularity | | x | x | | | x | | |
| M2 | Reusability | | x | x | | | x | | |
| M3 | Analyzability | | x | x | | | x | | |
| M4 | Modifiability | | x | x | | | x | | |
| M5 | Testability | | x | x | | | x | | |
| **S** | **Security** | **x** | **x** | **x** | | **x** | **x** | **x** | **x** |
| S1 | Confidentiality | x | x | x | | | x | x | x |
| S2 | Integrity | | x | x | | | x | x | x |
| S3 | Non-repudiation | x | x | | | x | | x | x |
| S4 | Accountability | x | x | | | x | | x | x |
| S5 | Authenticity | | x | | | | | x | x |

**Define responsibilities.** Define the responsibilities of all individuals participating in the assessment including the stakeholders, assessors, local assessment coordinator and participants.

**Identify ownership of the assessment record** and the person responsible for approving the assessor logs.

**Identify any additional information** that the stakeholders requests to be gathered during the assessment.

**Review all inputs.**

**Obtain stakeholders approval** of inputs.

## 3.2 Planning the Assessment

### *3.2.1 Overview*

An assessment plan describing all activities performed in conducting the assessment is developed and documented together with an assessment schedule. Using the project scope, resources necessary to perform the assessment are identified and secured. The method of collating, reviewing, validating and documenting all of the information required for the assessment is determined. Finally, co-ordination with participants in the Organization is planned.

### *3.2.2 Tasks*

**Determine the assessment activities.** The assessment activities will include all activities described in this documented assessment process but may be tailored as necessary.

**Determine the necessary resources and schedule for the assessment**. From the scope, identify the time and resources needed to perform the assessment. Resources may include the use of equipment such as overhead projectors, etc.

**Define how the assessment data will be collected, recorded, stored, analyzed and presented** with reference to the assessment checklist.

**Define the planned outputs of the assessment.** Assessment outputs desired by the stakeholders in addition to those required as part of the assessment record are identified and described. The output should have in consideration the stakeholder's background, board members or high-level management might want a simple output which shows the present state and which preservability characteristics need improvement. Technical stakeholders might want a detailed feedback on each of the characteristics.

**Manage risks.** Potential risk factors and mitigation strategies are documented, prioritized and tracked through assessment planning. All identified risks will be monitored throughout the assessment. Potential risks may include changes to the assessment team, organizational changes, changes to the assessment purpose/scope, lack of resources for assessment, confidentiality, priority of the data, and availability of key work products such as documents.

**Co-ordinate assessment logistics with the Local Assessment Coordinator**. Ensure the compatibility and the availability of technical equipment and confirm that identified workspace and scheduling requirements will be met.

**Review and obtain acceptance of the plan.** The stakeholders identify who will approve the assessment plan. The plan, including the assessment schedule and logistics for site visits is reviewed and approved.

**Confirm the stakeholders' commitment to proceed with the assessment.**

## 3.3 Briefing

### *3.3.1 Overview*

Before the data collection takes place, the Assessment Team Leader ensures that the assessment team understands the assessment input, process and output. The Organization is also briefed on the performance of the assessment.

### *3.3.2 Tasks*

**Brief the assessment team.** Ensure that the team understands the approach defined in the documented process, the assessment inputs and outputs, and is proficient in using the assessment tool.

**Brief the Organization.** Explain the assessment purpose, constraints, and process. Stress the confidentiality policy and the benefit of assessment outputs. Present the assessment schedule. Ensure that the staff understands what is being undertaken and their role in the process. Answer any questions or concerns that they may have. Potential participants and anyone who will see the presentation of the final results should be present at the briefing session.

## 3.4 Data Collection

### *3.4.1 Overview*

Data required performing the assessment is collected in a systematic manner. The strategy and techniques for the selection, collection, analysis of data and justification of the results are explicitly identified and demonstrable. The objective evidence gathered for each criterion assessed must be sufficient to meet the assessment purpose. Objective evidence that supports the assessors' judgment of the criteria compliance is recorded and maintained in the Assessment Record. This Record provides evidence to substantiate the results and to verify compliance with the requirements.

### *3.4.2 Tasks*

**Collect evidence of compliance for each criterion**.

**Record and maintain the references to the evidence** that supports the assessors' judgment of the characteristic assessment.

**Verify the completeness of the data.** Ensure that for each characteristic assessed, sufficient evidence exists to meet the assessment purpose.

## 3.5 Data Validation

### *3.5.1 Overview*

Actions are taken to ensure that the data is accurate and sufficiently covers the assessment purpose, including seeking information from first hand, independent sources; using past assessment results; and holding feedback sessions to validate the information collected. Some data validation may occur as the data is being collected.

### *3.5.2 Tasks*

**Assemble and consolidate the data.** For each characteristic, relate the evidence to the criterion.

**Validate the data.** Ensure that the data collected is correct and objective and that the validated data provides complete coverage of the assessment purpose.

## 3.6 Analysis of the Preservability Assessment

### *3.6.1 Overview*

For each characteristic, a percentage of compliance is calculated based on the evidence provided by the Organization. Traceability shall be maintained between the objective evidence collected and the percentages calculation.

### *3.6.2 Tasks*

**Establish and document the decision-making process used** to reach agreement on the results (e.g. consensus of the assessment team or majority vote).

**Record the set of percentages for all of the preservability characteristics and calculate the preservability status** of the system.

## 3.7 Reporting the Results

### *3.7.1 Overview*

During this phase, the results of the assessment are analysed and presented in a report. The report also covers any key issues raised during the assessment such as observed areas of strength and weakness and findings of high risk.

### *3.7.2 Tasks*

**Prepare the assessment report.** Summarise the findings of the assessment, highlighting the key results, observed strengths and weaknesses, and potential improvement actions (if within the purpose of the assessment).

**Present the assessment results to the participants.** Focus the presentation on defining the state of the preservability characteristics.

**Present the assessment results to the stakeholders.** The assessment results will also be shared with any parties (e.g. Organization management, practitioners, etc.) specified by the stakeholders.

**Finalize the assessment report** and distribute to the relevant parties.

**Verify and document that the assessment was performed according to requirements.**

**Assemble the Assessment Record.** Provide the Assessment Record to the stakeholders for retention and storage.

**Prepare and approve assessor records.** For each assessor, records to prove the participation in the assessment are produced. The stakeholders or the stakeholders' delegated authority approves the records.

**Provide feedback from the assessment** as a means to improve the assessment process.

# 4. ASSESSMENT RESULTS

The Civil Engineering Institution owns and maintains a system for supporting the process of acquiring and managing information captured from sensors installed in dams, with the objective of

studying the structure behavior and thus prevents any accidents that might happen. Besides managing sensor information, the system, which is called *DamMangement*, is also used for managing the visual inspections, physical models, mathematical models, and technical documents. It also provides data analysis tools such as tabular and chart reports and graphical representation of geo-referenced information.

The *DamMangement* System has the following features:

- Instrumentation: It integrates new observation instruments, supports the dynamic management of new types of instruments, and manages metadata about instruments.
- Transformation process: It manages the instrument specific algorithms to convert raw data into physical actions (results), using instrument metadata properties, such as calibration constants.
- Management of types of observations: It manages geodetic data information, information concerning visual inspections, and data provided by the automatic monitoring systems.
- Data visualization and exploitation: It accesses data through a set of reports designed to support the required types of data analysis, and spatially depicts data using a set of graphics and diagrams.
- Synchronization: It allows the deployment of the system in one or more locations (for example, Civil Engineering Institution and a dam owner) and the corresponding synchronization of data.

This section depicts the detailed assessment results and analysis for the Civil Engineering Institution's *DamMangement* system.

The detailed assessment results are depicted by Figure 2 and Figure 3. These show the results from different levels of detail. The first shows an overview of the different characteristics of preservability, while the second figure shows the in-depth results of each of the sub-characteristics of preservability. Such detailed results are useful for technical stakeholders as it gives a detailed insight on the current state of the different characteristics and sub-characteristics of preservability. The labels for Figure 2 and Figure 3 are shown in Table 3.

**Table 3: Charts Label**

| ID | Name | ID | Name |
|---|---|---|---|
| C | Compatibility | M3 | Analyzability |
| C1 | Co-Existence | M4 | Modifiability |
| C2 | Interoperability | M5 | Testability |
| P | Portability | S | Security |
| P1 | Adaptability | S1 | Confidentiality |
| P2 | Installability | S2 | Integrity |
| P3 | Replaceability | S3 | Non-repudiation |
| M | Maintainability | S4 | Accountability |
| M1 | Modularity | S5 | Authenticity |
| M2 | Reusability | | |

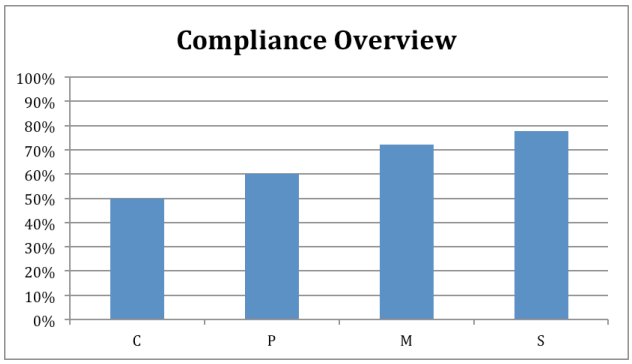


**Figure 2: Compliance Overview Results**

In Figure 2, the compliance overview of each of the characteristics is depicted, for the assessed case. The Civil Engineering Institution already has a high degree of security and also a high degree of maintainability, which means that the *DamMangement* system is highly maintainable and secure. Regarding compatibility and portability, the results are lower which might mean that system might not be prepared to be ported into a future environment and that it has not been tested with different components to check for compatibility issues. In Figure 3, we can depict the detailed results for each of the sub-characteristics of preservability. The sub characteristics are now described in increasing detail.

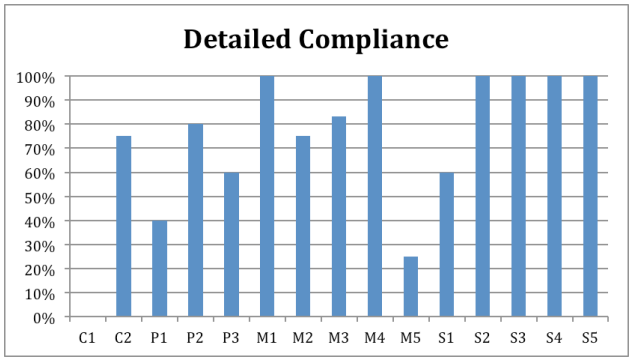


**Figure 3: Detailed Compliance Results**

## 4.1 Compatibility Sub-characteristics

The C1 sub-characteristic (Co-existence) could not be found in the *DamMangement* system which means that there is no list of known compatibility and incompatibility issues and there is no mechanism to check for dependencies and errors are not analysed for dependencies issues. The lack of this information might difficult the preservation actions to be taken on the system, since when preserving the system all its dependencies have to be accounted for. The compatibility information is especially important when there is a need for replacing certain components of the system when preserving or redeploying, in the case some original component is/becomes unavailable.

Regarding sub-characteristic C2 (Interoperability), the result attained was almost 80% which shows that *DamMangement* has data transformation mechanisms, it saves all input and output data used in these transformation mechanisms, has documentation about protocols and the interfaces are specified. For preservability, this is a particularly important fact, since data can be migrated to preservation friendly formats, or in future

redeployment scenarios, the system can more easily interoperate with future systems. However, *DamMangement* also uses external or proprietary protocols that might endanger the preservability status of *DamMangement* due to the possibility that these protocols become obsolete.

## 4.2 Portability Sub-Characteristics

The P1 sub-characteristic (Adaptability) reached 40% of compliance, which means that system already has some degree of adaptability. There is a list of issues concerning the system and software/hardware environments, and the system makes use of open source components, but on the other hands also makes use of proprietary components, which might be troublesome in redeployment scenarios where adaptations to the code have to be made in order to be able to run the system.

The P2 sub-characteristic (Installability) reached 80% of compliance, which shows that *DamMangement* doesn't have any external dependencies in the installation process. The existence of automatic installation packages, the existence of documentation on the resources needed to install the system, and the existence of installation documentation for the system, might contribute to make future installations of the system easier.

The P3 sub-characteristic (Replaceability) reached 60% of compliance, which depicts that in *DamMangement* there is an effort to maintain the system's interface clear so that a replacement would not jeopardise the system functionality. There is also an effort to use the same communication protocols throughout the whole system, when possible. Finally, the system's components are encapsulated in way that facilitates replacement efforts.

## 4.3 Maintainability Sub-characteristics

In the Maintainability characteristic, the M1 sub-characteristic (Modularity) reached 100% of compliance, which shows that the system has a modular design and that the coupling between modules is low. This is particularly important in preservation and redeployment scenarios where an original component is not available.

The M2 sub-characteristic (Reusability) reached almost 80% of compliance that shows that external interfaces are clearly specified, communication is standardized and the legal regulations in use permit reusability. This contributes for making the redeployment and reuse of a system easier and more trouble free.

The M3 sub-characteristic (Analysability) reached more than 80% of compliance which shows that the system's components have mechanisms which supports analysis, the system is also free from obfuscation techniques, it is implemented according to best practices and standards, is also implemented using popular technology and legal regulations permit analysis.

The M4 sub-characteristic (Modifiability) reached 100%, which shows that *DamMangement* is configurable and that legal regulation allow for modifications to the system, which is crucial so that the system can be configured and modified to adapt to whatever circumstances found in future environments.

The M5 sub-characteristic (Testability) only reached 25%, which shows that the system only allows to be tested without affecting the state of the system. This fact particularly jeopardizes the preservation of the sensor acquisition processes being supported by the system since it might be desirable to test the transformations made to sensor readings in the processes and if the redeployed system is able to provide the same results.

## 4.4 Security Sub-characteristics

In the Security domain, the S1 sub-characteristic (Confidentiality) reached 60% of compliance that shows that the system allows the specification of access rights to resources, implemented through authorization mechanisms, such as access control lists. It also shows that the system includes encryption mechanisms that might endanger preservability, and manages encrypted information, which can also endanger preservability if the encryption keys are not available in the future.

Regarding the S2 sub-characteristic (Integrity) *DamMangement* reached 100% of compliance that shows that the system includes integrity mechanisms and performs regularly scheduled integrity verifications. This fact is particularly important since it guarantees that the data that is going to be preserved along with the system is not compromised.

The S3 sub-characteristic (Non-repudiation) reached 100% of compliance that depicts that the system has mechanisms for producing records of actions and actively produces records of actions or events on data or components. This fact is particularly important since it ensures that any changes to the system or data are registered, ensuring provenance.

The S4 sub-characteristic (Accountability) reached also 100% of compliance which shows that the system produces records of actions or events on data or components associated with the entities the performed them. This fact is particularly important since it ensures that any changes to the system or data are registered, ensuring provenance.

Finally, the S5 sub-characteristic (Authenticity) reached 100% of compliance that shows that the system has mechanisms for enforcing the authenticity of the entities accessing the system and the system actively enforces the authenticity of the entities accessing the system, thus guaranteeing authentic system components and data.

These results can be used by technical stakeholders to enhance the *DamMangement* system and guarantee that the system is preservable in the future. According to the results, the stakeholders might want to focus the enhancement efforts in the compatibility and portability characteristics.

# 5. CONCLUSION AND FUTURE OUTLOOK

This paper aimed at the development of a preservability assessment method based on the hypothesis that preservability is a set of systems capabilities originating from a combination of system/software qualities.

An assessment method was proposed to take into account the specifics of each scenario, taking into account the state of the art in assessment checklists and standards on assessment processes. For validating this method, an assessment was performed on the Civil Engineering Institution use case, involving the gathering of the requirements of the stakeholders of the case and the creation of a checklist for assessing preservability in this specific case. The main findings are that the preservability degree of the system described in the industrial case is satisfactory. However, these results can be improved if the documentation concerning some aspects is created and, when existing, that it is kept up to date. Another aspect that can cause preservability to be improved is to keep a registry of compatibility information and performing regular analysis of the compatibility of the system and its components.

The work presented in this paper is not definitive. In fact, it is a proof-of-concept that needs to mature with the application and validation using different scenarios. The example application of the method to the Civil Engineering Institution use case used a checklist where each criterion has a binary evaluation (yes/no), which allows only making limited conclusions. In fact, the desired scenario would be the evaluation of each criterion in a quantitative/qualitative fashion and the creation of a maturity model for preservability against which the evaluation results would be matched. Such scenario is only possible after the application and validation of the method and technique used to several different scenarios which could be used as a benchmark for the creation of the maturity levels.

## 6. ACKNOWLEDGMENTS

This work was supported by national funds through FCT – Fundação para a Ciência e Tecnologia in context of the pluriannual project PEst-OE/EEI/LA0021/2011, by the project TIMBUS, co-funded by the EU under FP7 under grant agreement no. 269940, and by COMET K1, FFG – Austrian Research Promotion Agency.

## 7. REFERENCES

[1] ISO/IEC 25010 - Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models, International Organization for Standardization and International Electrotechnical Commission Std. 2010

[2] ISO/IEC 15504 - Information technology — Process assessment, International Organization for Standardization and International Electrotechnical Commission Std. 2004.

[3] IT Governance Institute. COBIT 5 – A business Framework for the Governance and Management of Enterprise IT. 2012.

[4] RWTH i* Guide, [online] http://istar.rwth-aachen.de/tiki-index.php?page=i%2A+Guide&structure=i%2A+Guide (Accessed on 25.02.2013).

[5] IT Governance Institute. *COBIT 5 – Enabling Processes.* 2012.