# Digital Quality Monitoring and Compliance Management for Critical Industrial Security Infrastructure under Saudi Vision 2030.


## Abstract

Industrial security infrastructure must be commissioned with evidence that its physical assets, digital configuration and operating interfaces satisfy approved requirements. Fragmented work records can obscure missing compliance evidence. This paper proposes a framework for linking controlled requirements, asset identities, test evidence, exceptions and authorized release decisions. It draws on a structured narrative review of digital construction, rule checking, information management and operational technology governance, alongside public Saudi policy and control documents. A hypothetical industrial facility illustrates how to verify a cross-package interface and preserve a usable record after handover. The paper proposes measurements for evidence integrity, workflow timeliness and the reliability of compliance decisions. The framework supports Saudi Vision 2030 through auditable delivery and local capability. Its performance and organizational burden require evaluation on authorized projects.



**Keywords** Industrial security infrastructure, digital quality monitoring, compliance evidence, operational technology, digital handover, Saudi Vision 2030



UNDER PEER REVIEW IN IJAR


## 1. Introduction

Industrial security infrastructure includes physical assets, supporting services, digital equipment and interfaces that must work together after construction. Quality monitoring typically tracks installation, inspection and commissioning. Compliance management connects the verified condition of those assets to an applicable requirement and an accountable decision. When the two processes use separate registers, a dashboard may show high construction completion even though the organization cannot establish that the approved configuration, completed tests and current requirements refer to the same asset.

Consider an asset with an accepted installation and an approved record of functional testing. If a later configuration change alters the basis of that test, the digital record should show which evidence remains applicable and which test needs review. A report that treats every uploaded file as evidence of current compliance will miss this distinction. The risk increases when the party that uploads construction records leaves the project before operations staff have learned how to retrieve and interpret them.

Saudi Vision 2030 and its industrial development programs provide the strategic setting. Reliable industrial operations depend in part on the ability to demonstrate what was installed, establish a handover baseline and control later changes. Public Saudi cybersecurity controls and applicable industrial security requirements may govern different aspects of a project. Applicability needs confirmation by the asset owner with the appropriate parties. A strategic

program, a public control document and a project-specific acceptance criterion have different authority and need different treatment within the assurance record.

### 1.1Aim and objectives

The aim is to propose a digital quality monitoring and compliance management framework for critical industrial security infrastructure construction and handover. The objectives are to define a structured evidence chain, identify decisions suitable for automated checking, specify controls for sensitive project information, design a process for managing exceptions and propose a method for evaluating the framework. The intended audience includes owners, commissioning managers, construction quality teams and assurance personnel.

### 1.2Research questions

How can a project connect requirements, verified assets and evidence across contractors and revisions? Which parts of compliance checking can be automated with reliable inputs and which require professional judgment? How can a project protect sensitive records while giving reviewers enough information to make an accountable decision? What evidence would show that digital monitoring improves compliance decisions and handover quality?

## 2. Review methodology

A structured narrative review combines research on building information modelling, construction digital twins, automated rule checking and data integration with public guidance on security-minded information management and operational technology. Sources were selected to address three practical issues. The first is representation of what the owner requires. The second is evidence that installed assets and configurations satisfy those requirements. The third is protection and preservation of records that describe sensitive infrastructure.

The review separates empirical studies, design literature, standards and public policy documents. Research on model integration informs the evidence architecture. Standards and public controls inform governance questions within their published scope. The paper does not reproduce protected facility details or infer an installation specification from general cybersecurity guidance. A hypothetical example checks whether the proposed workflow covers construction, commissioning and subsequent changes. The example uses no observed incident, facility configuration or measured project outcome.

## 3. Thematic review and critical analysis

### 3.1Information models and asset identity

Building information modelling can provide a spatial and object-oriented index into project information. A digital twin can add continuing links to observations or operational states where its use justifies the effort. Neither representation supplies trustworthy compliance evidence by itself. A model object may still show a generic component after procurement, while a test record refers to an installed device with a distinct identifier. The relationship between design intent and installed identity must be verified rather than assumed from a shared drawing location.

UNDER PEER REVIEW IN IJAR

Research on existing asset models highlights missing records and inconsistent levels of detail. The challenge matters before handover as well. Replacements, splits and combinations can change asset identity even while the model geometry remains stable. A single identifier should have a defined creation point and owner. Where the owner's operational numbering differs from the construction system, a controlled mapping should record the transition and preserve access to the historical evidence.

Information requirements should reflect decisions the owner expects to make. Collecting detailed attributes that operations never use adds reconciliation work. Conversely, a small omission such as the absence of an approved configuration reference can prevent later interpretation of a successful test. The essential question is which information supports an accountable decision at a specified stage, who confirms it and how long it must remain available.

## 3.2Automated rules and professional judgment

Automated checking can reliably verify some relationships when the data model and rule are explicit. Examples include detecting a missing required record, finding an expired approval date or identifying a test attached to a superseded revision. More complex checks may require geometric reasoning or interpretation of a condition that is rarely structured consistently. Rules should record their prerequisites and return an unresolved status when those prerequisites are missing.

A digital flag can trigger a review. It cannot establish the intended meaning of a contract clause or resolve conflicting authority. Some requirements concern how several components function under a defined test condition. Evaluating them involves observation, technical judgment and approval by a designated person. A rule engine can verify that the approved test was linked and signed, while the technical decision remains with the responsible reviewer.

Versioning is central to reproducibility. If the team changes an automated rule after commissioning, a later check may produce a different result for unchanged evidence. The historical record should preserve the rule version, input snapshot and decision issued at the time. A second evaluation can apply the updated rule and show the difference. This supports controlled reassessment when an owner updates requirements or discovers an error in the rule.

## 3.3Security-minded handling of evidence

Construction and commissioning records can describe the physical and digital arrangements of a facility. Sharing them broadly may expose information unnecessary for a recipient's role. Restricting every record equally can also slow review and encourage informal copies. Information classification should distinguish the sensitivity of source evidence, derived results and the relationships created when records are combined.

Operational technology guidance emphasizes dependable operations and controlled changes. The assurance platform can consume authorized reports or approved extracts without direct access to production systems. In a commissioning workflow, collection methods should be agreed with the facility owner. Testing and monitoring should follow authorized procedures and preserve safe operating conditions. Public cybersecurity guidance can help establish

UNDER PEER REVIEW IN IJAR

governance principles, with the owner determining how applicable requirements enter the project baseline.

# 4. Proposed compliance framework

## 4.1Establish the applicability register

The owner maintains an applicability register identifying each requirement, its source and revision, the scope to which it applies, the designated authority and the evidence needed. Record whether the requirement comes from law, regulator, contract, approved design or an internal procedure. Retain the basis for applicability and how conflicts or overlaps were resolved. The person administering a dashboard should have a route to escalate interpretation to the responsible authority.

Each requirement receives an identifier stable enough to follow through design, procurement, installation, testing and handover. If the source changes, the project should preserve the prior revision and record when the new revision begins to govern. The review identifies affected assets, test procedures, procurement commitments and approvals already issued. This prevents a change in the register from giving the appearance of retroactive verification.

Some requirements apply at a system level and others at component level. A system requirement may depend on several component results plus an integrated test. The compliance record should represent the dependency explicitly. Completion of component records can satisfy a prerequisite without closing the system requirement. The authority for release reviews the combined evidence at the appropriate stage.

## 4.2Structure the evidence and decisions

The minimum evidence record contains the requirement identifier, asset or system identity, location scope, revision, method or procedure, test date, result, originator and disposition. Evidence references are durable links to controlled records. Supporting artifacts can be stored in restricted repositories, with the main register retaining the authorized reference and enough metadata for an assigned reviewer to verify it. Each decision should indicate the specific evidence on which it relies.

Separate record availability from technical acceptance. A document can be present and pending review. A reviewed record can be incomplete for the decision because it covers a different item or configuration. Statuses can distinguish evidence missing, submitted, reviewed, accepted, rejected and superseded. An approved exception needs a separate state, since the owner may allow limited progression while still requiring follow-up action.

A single closure event should be attributable to an authorized role, with the decision and conditions retained. When the project changes an item, it should identify which downstream decisions are affected and which can remain in force. For example, replacing equipment can invalidate a functional test without affecting a civil measurement. Keeping the evidence granular avoids both unnecessary retesting and accidental reuse of an obsolete result.

UNDER PEER REVIEW IN IJAR

## Table 1. Evidence and responsibility at each stage

| Stage | Required evidence | Decision owner |
|---|---|---|
| Applicability | Source, revision, scope and basis for inclusion | Requirement owner confirms applicability. |
| Installation | Asset identity, approved revision and inspection result | Authorized inspector verifies the installed condition. |
| Commissioning | Controlled configuration and approved functional test result | Release authority reviews the combined evidence. |
| Handover | Current baseline, approved exceptions and evidence links | Operations confirms custody and retrieval. |

### 4.3Manage exceptions and release

Exceptions are assigned a responsible owner, technical basis, authorized decision, affected scope and review or expiry date as applicable. The project records dependencies that prevent full release. An engineering disposition may allow progression within a defined boundary while an unresolved item remains visible. A dashboard should show the difference between conditional permission and full satisfaction of a requirement.

If an exception is overdue, the escalation should reach the owner of the decision and any function relying on it. Updating the date requires an authorized reason. Overdue items should remain visible in historical reporting even if later resolved. Otherwise the project loses evidence of the time during which the exposure remained open.

A release review starts from the intended use of the asset or system. It verifies that the applicable evidence is current and that unresolved items have the necessary disposition. Reviewers can use a status summary to locate priority items and should have authorized access to underlying records. A compliance report generated for an external audience should contain the level of detail approved for that purpose.

### 4.4Protect and preserve records

A role model assigns appropriate access to contractors, owner representatives, auditors and operations staff. A reviewer needs enough information to decide the item in scope, and the system should restrict unrelated sensitive evidence. Sensitive files should follow the owner’s approved storage and distribution rules. Logs record important changes and access events at a level that supports investigation and accountability.

The owner also needs continuity when a repository or contractor platform changes. Specify exportable identifiers, versions, decision records and attachment references as part of procurement. Test an authorized retrieval and recovery workflow before handover. An export that contains names of attachments but loses their link to the decision may be insufficient to demonstrate what was accepted. Retention should follow applicable contractual and organizational rules.

When field connectivity is limited, inspectors may capture authorized records through a controlled offline process. The process should preserve identity, timestamps, revisions and

UNDER PEER REVIEW IN IJAR

responsibility when records are synchronized. Duplicate submissions should be reconciled without overwriting the original decision history. A failed synchronization should be visible and handled before affected records are treated as available for release.

### 4.5Define the operating model for assurance

An effective compliance record depends on a clear assignment of authority. The requirement owner interprets the source and confirms applicability. The evidence producer completes the authorized inspection or supplies the controlled record. The reviewer checks that the evidence supports the decision, and the release authority accepts responsibility for allowing the next stage. A project can combine roles where appropriate, but the recorded decision should still show who performed each function. Critical decisions may require separation under the owner's governance.

The program needs an escalation route for cases that cross boundaries. An interface issue can involve physical construction, networked equipment and operating procedures, with each package able to resolve only part of the issue. The owner should establish a shared issue identifier and assign an authority who can coordinate the necessary decisions. Where one part of the work can progress independently, the permission should describe the boundary and evidence supporting that separation.

The project should also define a point at which operations assumes ownership of the evidence. During turnover, there may be an interval in which the construction organization still corrects defects while operations authorizes changes. A transition plan can identify which system is authoritative for each record type, who reviews new evidence and how remaining exceptions are transferred. An unresolved item should retain its age and technical history when ownership changes.

## 5. Illustrative application

### 5.1Commissioning across three work packages

Consider a hypothetical Saudi industrial site where civil works, equipment installation and systems integration are delivered by different contractors. The owner defines a generic functional requirement that a specified facility subsystem must demonstrate the approved operating response during an authorized commissioning test. The equipment installation package verifies the physical items and records their asset identifiers. The integration contractor submits a test against an approved configuration baseline. The owner retains a record of which results support the integrated requirement.

During the review, a digital rule flags that the configuration identifier on the test report differs from the approved baseline. The flag is evidence of an inconsistency in the records. The reviewer determines whether the difference is a clerical error, an authorized configuration revision or a real mismatch requiring further work. The approved release route depends on that assessment. The register preserves the flag, the review and any new evidence, including the outcome of an authorized retest if required.

Later the owner accepts the integrated test and prepares handover. The operations team receives an approved baseline, the required evidence references and any authorized

UNDER PEER REVIEW IN IJAR

exceptions. A retrieval exercise asks a reviewer to reconstruct the chain from requirement to disposition and find the controlled record behind it. The exercise exposes whether a third-party platform login, expired link or unavailable attachment would prevent the owner from using the evidence.

### 5.2Change after handover

Suppose an equipment item is replaced during authorized maintenance. The operations team records the new identity and change approval. The evidence chain identifies which earlier decisions depended on the replaced item. The owner determines which records remain valid and which need renewed verification. The prior baseline remains available for interpreting the original handover and earlier operating history.

This example shows why the compliance record needs a change workflow even after construction closes. A handover archive preserves history. A controlled operational register maintains the relationship between current equipment, approved changes and continuing assurance. The two can be linked without requiring all operating data to be duplicated in the construction system.

## 6. Evaluation design

### 6.1Measures of evidence and decision quality

Evidence completeness is the share of eligible requirements with all necessary evidence types linked and available for review at a given stage. Technical acceptance is tracked separately. A reviewer can therefore distinguish delayed submission from a failure of the work to satisfy the approved test. Report the measures by stage and criticality, since a high overall figure can conceal a small set of consequential unresolved items.

Decision reliability can be assessed through independent review of a sample of closures. A false closure occurs when the evidence available at the recorded time does not support the assigned status. Reviewers should document whether the cause was missing evidence, an invalid rule, an identity mismatch or an unauthorized disposition. To interpret the sample, disclose the selection method and the number of cases reviewed, particularly if critical items are oversampled.

Operational measures include time to locate required evidence, time from complete submission to disposition and the duration of unresolved critical exceptions. Include workflow burden, such as duplicate entries or additional review hours, as a balancing measure. Teams should record outages and synchronization delays because they affect both data completeness and the apparent speed of decisions.

UNDER PEER REVIEW IN IJAR

## Table 2. Illustrative status at a commissioning gate

| Status | Count | Share of 200 eligible records |
|---|---|---|
| Accepted | 170 | 85% |
| Pending technical review | 14 | 7% |
| Rejected | 6 | 3% |
| Evidence missing | 10 | 5% |

Evidence is available for 190 of 200 requirements. Technical acceptance covers 170. A critical unresolved requirement can still prevent release under the approved procedure.

### 6.2Pilot and acceptance criteria

Start with one system or work package with repeatable requirements and a clear owner. Record a baseline using the current process. Run the digital register alongside existing procedures for a defined period and compare results on matched requirements or controlled test cases. Deliberately seed safe record discrepancies in a test environment, such as an expired evidence link or duplicate identifier, to verify that the rule engine flags them correctly.

Before deployment, agree on criteria for accurate flagging, unauthorized closure prevention, evidence retrieval and recovery after service interruption. Test whether authorized staff can perform essential decisions when the platform is unavailable, then reconcile temporary records through an approved process. These tests evaluate continuity of the assurance workflow rather than the security performance of the facility.

A follow-up study can compare similar work packages under ordinary and digitally supported processes. Reviewers should use a shared definition of completeness, scope and false closure. The analysis should record major changes in team composition or procurement because they can affect outcomes independently of the framework. Where the sample is limited, report descriptive results and investigate the causes of discrepant cases.

### 6.3Validate automated checks with safe test records

Rule validation can start with a small synthetic dataset that contains expected passing, failing and unresolved cases. Include an item with a valid test under the wrong revision, an approval from an unauthorized role and a legitimate case with a missing prerequisite field. The owner should retain the expected result for each test. If a software update changes the result, the test provides a reproducible basis for investigation.

After initial validation, review a sample of decisions made under live procedures. Reviewers can compare the rule output with the controlled evidence without exposing sensitive details beyond their remit. Report errors in both directions. A false flag wastes review time and can delay release, while a missed flag can leave an inconsistency undetected. Performance depends on the completeness and quality of the inputs as well as the logic of the rule.

A validation record should identify the rule author, technical approver, version and date brought into use. When a requirement is withdrawn or changed, retire or revise the associated

UNDER PEER REVIEW IN IJAR

check through the same process. Older rule definitions remain useful for explaining decisions already made. This version trail supports review when a project discovers that the correct interpretation was available only after an earlier commissioning period.

# 7. Discussion

The proposed architecture can be implemented with a controlled register and repository before the project invests in a model viewer or real-time interface. The biggest gains may come from consistent asset identity and documented authority. More advanced tools become useful when they address specific problems such as dependencies among systems or slow retrieval of distributed evidence. Owners can compare the cost of integration with the reduction in search time, duplicate work or unresolved handover items.

A major trade-off concerns visibility and sensitivity. Senior managers need enough information to intervene when critical assurance is delayed. The underlying technical detail may require restricted handling. A layered dashboard can show decision status and exposure to an authorized management group while limiting detailed evidence to reviewers with a defined role. Testing each view with representative users can expose both unnecessary disclosure and access restrictions that prevent legitimate work.

For Saudi industrial development, the most direct alignment is the ability to deliver industrial assets with usable evidence and sustain assurance locally. An owner can require that local assurance staff participate in rule validation, change review and handover exercises. Procurement can specify continuity when vendor support changes and require evidence exports that preserve context. The paper treats these as project capabilities that may support wider industrial goals when sustained across multiple facilities.

## 7.1Plan for institutional continuity

Long-term ownership includes maintaining reference data, controlling permissions and reviewing changes to the evidence platform. A practical owner’s manual can describe who may create asset identities, how new contractors receive access and which operating function maintains the requirement register after handover. These decisions become important when multiple facilities adopt the same framework under different local arrangements.

Training can use synthetic or appropriately authorized examples that show how to reconstruct a decision. A competency exercise should ask a reviewer to locate the applicable requirement, identify the valid evidence and explain the recorded disposition. Completing the exercise demonstrates the ability to use the assurance chain under realistic conditions. Training statistics alone give less insight into whether the evidence remains usable.

Program-level learning can use aggregated measures and de-identified examples when approved. Facilities can compare evidence retrieval time, data completeness and recurring causes of false closure without exchanging unnecessary details. A common set of definitions allows a Saudi industrial owner to identify where a procurement clause, training activity or rule clarification could improve several projects. The framework’s contribution depends on whether that feedback reaches the people who own those decisions.

UNDER PEER REVIEW IN IJAR

# 8. Limitations and future research

The narrative review does not produce a statistical estimate of effectiveness. Detailed facility requirements and incident data may be restricted, limiting public replication and comparison. The hypothetical scenario tests the logic of the workflow and supplies no evidence of regulatory approval or security performance. Organizations should establish applicability and technical acceptance within their authorized project arrangements.

Future research should examine inter-reviewer agreement, the cost of maintaining automated rules and the durability of evidence after contractor transition. A controlled comparison could test whether evidence retrieved through a structured register remains interpretable longer than evidence filed by package alone. Further research should assess how to preserve confidentiality while enabling independent evaluation using synthetic records or aggregated results approved for release.

# 9. Conclusion

Digital quality monitoring supports industrial security compliance when it connects applicable requirements to verified asset identities, current evidence and authorized decisions. The proposed framework assigns explicit responsibilities for applicability, automated checks, exceptions, record protection and handover. The illustrative case shows how a revision discrepancy can be caught before it becomes an unsupported release decision. A controlled pilot would measure decision reliability, retrieval time and workload. Those measures provide a practical basis for determining whether the framework improves the delivery and continuity of industrial assurance in the Saudi Vision 2030 context.

# References


Akinci, B., Boukamp, F., Gordon, C., Huber, D., Lyons, C., & Park, K. (2006). A formalism for utilization of sensor systems and integrated project models for active construction quality control. Automation in Construction, 15(2), 124–138. https://doi.org/10.1016/j.autcon.2005.01.008

Boje, C., Guerriero, A., Kubicki, S., & Rezgui, Y. (2020). Towards a semantic construction digital twin. Directions for future research. Automation in Construction, 114, 103179. https://doi.org/10.1016/j.autcon.2020.103179

Eastman, C., Lee, J.-M., Jeong, Y.-S., & Lee, J.-K. (2009). Automatic rule-based checking of building designs. Automation in Construction, 18(8), 1011–1033. https://doi.org/10.1016/j.autcon.2009.07.002

Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital twin. Enabling technologies, challenges and open research. IEEE Access, 8, 108952–108971. https://doi.org/10.1109/ACCESS.2020.2998358

International Electrotechnical Commission. (2013). Industrial communication networks — Network and system security — Part 3-3. System security requirements and security levels (IEC 62443-3-3:2013). https://webstore.iec.ch/en/publication/7033


UNDER PEER REVIEW IN IJAR

International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022). https://www.iso.org/standard/27001

International Organization for Standardization. (2018). Organization and digitization of information about buildings and civil engineering works, including building information modelling — Information management using building information modelling — Part 1. Concepts and principles (ISO 19650-1:2018). https://www.iso.org/standard/68078.html

International Organization for Standardization. (2020). Organization and digitization of information about buildings and civil engineering works, including building information modelling — Information management using building information modelling — Part 3. Operational phase of the assets (ISO 19650-3:2020). https://www.iso.org/standard/75109.html

International Organization for Standardization. (2020). Organization and digitization of information about buildings and civil engineering works, including building information modelling — Information management using building information modelling — Part 5. Security-minded approach to information management (ISO 19650-5:2020). https://www.iso.org/standard/74206.html

International Organization for Standardization. (2026). Quality management systems — Requirements (ISO 9001:2026). https://www.iso.org/standard/9001

Kingdom of Saudi Arabia. (2016). Saudi Vision 2030. https://www.vision2030.gov.sa/en/

Kingdom of Saudi Arabia. (n.d.). National Industrial Development and Logistics Program. https://www.vision2030.gov.sa/en/explore/programs/national-industrial-development-and-logistics-program

Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W. (2018). Digital twin in manufacturing. A categorical literature review and classification. IFAC-PapersOnLine, 51(11), 1016–1022. https://doi.org/10.1016/j.ifacol.2018.08.474

Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001

National Cybersecurity Authority. (2022). Operational Technology Cybersecurity Controls (OTCC-1:2022). https://nca.gov.sa/en/regulatory-documents/controls-list/otcc/

National Cybersecurity Authority. (2024). Essential Cybersecurity Controls (ECC 2-2024). https://nca.gov.sa/en/regulatory-documents/controls-list/ecc/

National Cybersecurity Authority. (2024). Guide to Operational Technology Cybersecurity Controls implementation. https://cdn.nca.gov.sa/api/public/cms/files/0d563108-e1c6-43fd-bd4b-a0d5a22d83e8_OTCC_Implementation-Guideline_en.pdf

National Institute of Standards and Technology. (2006). Guide to computer security log management (SP 800-92). https://doi.org/10.6028/NIST.SP.800-92

UNDER PEER REVIEW IN IJAP

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2023). Guide to operational technology (OT) security (SP 800-82 Rev. 3). https://doi.org/10.6028/NIST.SP.800-82r3

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

Pauwels, P., Zhang, S., & Lee, Y.-C. (2017). Semantic web technologies in AEC industry. A literature overview. Automation in Construction, 73, 145–165. https://doi.org/10.1016/j.autcon.2016.10.003

Solihin, W., & Eastman, C. (2015). Classification of rules for automated BIM rule checking development. Automation in Construction, 53, 69–82. https://doi.org/10.1016/j.autcon.2015.03.003

Tang, S., Shelden, D. R., Eastman, C. M., Pishdad-Bozorgi, P., & Gao, X. (2019). A review of building information modeling (BIM) and the internet of things (IoT) devices integration. Present status and future trends. Automation in Construction, 101, 127–139. https://doi.org/10.1016/j.autcon.2019.01.020

Volk, R., Stengel, J., & Schultmann, F. (2014). Building information modeling (BIM) for existing buildings. Literature review and future needs. Automation in Construction, 38, 109–127. https://doi.org/10.1016/j.autcon.2013.10.023

UNDER PEER REVIEW IN IJAR