International Journal of BIM and Engineering Science

♦ ISSN: 2571-1075 Vol: 12, No. 02, 2026 ♦ PP. 57–65

Article DOI: https://doi.org/10.54216/IJBES.120208

FULL LENGTH ARTICLE

An Automated Framework for Integrating Crime Prevention through Environmental Design into BIM-Based Security Validation

Juli Yani[1,*] **Maisaroh Ritonga**[1] **Citra Dewi**[2]

[1] Universitas Al Washliyah Labuhanbatu, Indonesia

[2] Universitas Lampung, Indonesia

Emails: yanijuli90@gmail.com • ritongamaisaroh2@gmail.com • citra.dewi@eng.unila.ac.id

Received: January 09, 2025 Revised: February 28, 2026 Accepted: March 29, 2026 ⋆ Corresponding author

ABSTRACT

Security validation in architectural design is commonly conducted through manual interpretation of drawings, expert walkthroughs, and late-stage design reviews. Such practice is valuable but difficult to reproduce, especially when crime-prevention criteria depend on visibility, access definition, territorial cues, and lighting quality. This paper presents an automated BIM-based framework for evaluating Crime Prevention through Environmental Design (CPTED) principles using semantic modelling, geometric reasoning, and rule-based inference. The proposed method transforms security-relevant BIM entities into a machine-readable CPTED knowledge layer, evaluates each space through formal rules, and produces interpretable scores that can guide design revision. The framework considers natural surveillance, access control, territoriality, and lighting as computationally linked design dimensions rather than independent checklist items. Results show that automated rule checking can reproduce expert assessment patterns while providing faster and more consistent space-level diagnosis. The paper contributes a transparent computational model for early-stage security validation and demonstrates how BIM can support evidence-based CPTED assessment before construction decisions become costly to revise.

Keywords: Building information modeling ▪ CPTED ▪ Security validation ▪ Rule-based reasoning ▪ Knowledge graphs ▪ Spatial analysis

1. INTRODUCTION

Crime Prevention through Environmental Design (CPTED) has become an important design philosophy for reducing opportunities for crime through the organisation of physical space. Its principles encourage designers to improve visibility, control access, strengthen territorial cues, and remove environmental conditions that support concealment or ambiguous ownership. Although these principles are widely discussed in urban planning, facility management, and security engineering, their application in building design is still frequently carried out through manual drawings review, expert judgement, and narrative audit forms. This limits the consistency and timeliness of security feedback during early design development.

Building Information Modeling (BIM) offers a more structured basis for CPTED assessment because it contains spaces, doors, windows, walls, lighting devices, security assets, and circulation relationships in a computable form. A BIM model can be queried for adjacency, visibility, access points, and object properties that are directly related to CPTED concepts. However, this potential is not fully realised when BIM is treated only as a geometric repository. Security validation

requires a semantic layer that explains why a door, window, room, corridor, camera, or lighting fixture matters for a particular CPTED principle.

The main challenge is that CPTED guidance is often expressed in qualitative language, while automated BIM checking requires explicit rules, thresholds, and measurable features. For example, natural surveillance is normally described as the ability of legitimate users to observe a space, but a computational model must translate this idea into visibility ratios, window positions, camera support, and obstruction conditions. Similarly, access control is not limited to the number of doors; it also depends on whether entrances are controlled, whether restricted spaces are separated, and whether circulation paths create avoidable exposure.

This paper proposes a BIM-based CPTED validation framework that connects semantic knowledge representation, geometric feature extraction, and rule-based reasoning. The framework parses an IFC-oriented building extract, identifies security-critical entities, maps them to CPTED attributes, and computes a transparent security score for each space. The model is designed as a decision-support procedure rather than a black-box classifier: each score is traceable to rules, input attributes, and principle-level indicators.

The contribution of the paper is threefold. First, it formalises CPTED assessment as a computable BIM rule-checking problem using a spatial-knowledge representation. Second, it develops a scoring model that combines natural surveillance, access control, territoriality, and lighting into a space-level security indicator. Third, it evaluates the model through expert-comparison, ablation, sensitivity, clustering, and scenario analyses, demonstrating how the framework can be used as an iterative design tool for improving security performance.

2. CONCEPTUAL AND TECHNICAL BACKGROUND

CPTED research has long argued that crime and perceived safety are influenced by environmental features, including visibility, boundary definition, maintenance, activity support, and access organisation. Recent work has renewed attention to CPTED as a structured audit practice rather than a purely descriptive concept. Cozens and colleagues developed a CPTED audit tool through an ecological lens and emphasised the need for more systematic assessment processes [1]. Shach-Pinsly proposed spatial approaches for identifying secure and vulnerable spaces, supporting the idea that security assessment can be informed by measurable environmental characteristics [2]. These studies show that security design can be evaluated empirically, but they also reveal a gap between field audit methods and building-scale digital validation.

Public crime-environment datasets provide another important foundation. Azevedo et al. introduced the "Looking at Crime: Communities and Physical Spaces" dataset, which combines local security diagnosis, school-environment diagnosis, and physical-space observations [3]. Such datasets are useful because they demonstrate how CPTED-related physical observations can be organised for descriptive and inferential analysis. However, they are not directly connected to BIM models. This paper uses their logic as inspiration for structuring CPTED observations, while the assessment itself is performed on BIM-derived spaces and assets.

BIM-based automated compliance checking has advanced rapidly through semantic web technologies, knowledge graphs, and formal rule languages. Peng et al. proposed a BIM and knowledge-graph-based automated compliance checking system that transforms regulatory knowledge into computable semantic structures [4]. Patlakas et al. examined semantic-web-based automated compliance checking in the context of engineering computation [5], while Ma et al. presented ontology-based checking of BIM models against standards [6]. These works provide methodological support for representing CPTED requirements as rules over BIM data, although their primary emphasis is regulatory compliance rather than security-by-design validation.

IFC datasets and open BIM test models have improved reproducibility in BIM research. The TU Wien real-world escape-route model provides an IFC-based building model for validation of automated checking procedures [7], and the TUM GNI BIM dataset supplies a larger collection of anonymised IFC building models for method testing [8]. Such datasets demonstrate the feasibility of public BIM validation workflows. In the present paper, the experimental extract follows this open-model logic by representing spaces, doors, windows, cameras, lighting, and circulation conditions as computable BIM-like entities for CPTED scoring.

Security-related BIM studies also point to the value of structured information models. BIM has been studied for access-control policies, safety risk assessment, and facility-management security contexts. Lu et al. proposed BIM-integrated construction safety risk assessment at the design stage [9], demonstrating how design information can support quantitative risk reasoning. Brelih et al. discussed security and privacy concerns in BIM-enabled common data environments [10]. Although these works address safety and information security rather than CPTED scoring, they support the broader argument that BIM can carry security-relevant decision information across the lifecycle.

A key limitation in the existing literature is the lack of an integrated framework that turns CPTED principles into machine-readable BIM validation rules and then tests the resulting scores against manual assessment and design sensitivity. Most CPTED studies remain audit-based or spatial-analysis oriented, while BIM rule-checking studies usually focus on code compliance, accessibility, fire safety, or model quality. This paper addresses this gap by combining CPTED ontology mapping, BIM entity extraction, geometric and spatial indicators, expert-comparison validation, and design-parameter sensitivity into one reproducible framework.

3. SECURITY VALIDATION MODEL

The proposed model is organised around an explainable security-validation chain rather than a conventional compliance checklist. Its purpose is to convert CPTED concepts into measurable BIM-derived indicators while preserving the interpretability needed by architects, facility managers, and security consultants. The model receives an IFC-oriented spatial extract, constructs a CPTED knowledge layer, evaluates each space through principle-specific rules, and returns diagnostic scores that indicate where design revision is needed.

Table 1. Summary of verified studies and data sources related to BIM-CPTED security validation.

Ref.	Study focus	Methodological orientation	Main contribution	Relevance to this study
[1]	CPTED audit tool development	Ecological CPTED assessment	Developed a structured CPTED audit process	Supports rule organisation for CPTED assessment
[2]	Secure and vulnerable urban spaces	Spatial safety assessment	Defined spatial patterns of perceived safety and vulnerability	Motivates measurable spatial indicators
[3]	Crime and physical-space dataset	Curated observational data	Organised CPTED-related environmental observations	Supports data structure for CPTED evidence
[4]	BIM compliance checking	Knowledge graph and BIM	Converted building rules into semantic compliance checks	Supports knowledge-graph reasoning over BIM
[5]	Semantic automated compliance checking	Semantic web and engineering computation	Linked rule checking with computational methods	Supports formal rule validation
[6]	BIM standards checking	Ontology-based compliance checking	Proposed ontology-based BIM model quality assessment	Supports semantic representation of rules
[7]	TU Wien IFC validation model	Open BIM test model	Public IFC model for automated checking validation	Supports reproducible BIM validation context
[8]	TUM GNI BIM dataset	Open IFC model collection	Large IFC dataset for method validation	Supports cross-building testing potential
[9]	BIM-based safety risk assessment	Design-stage quantitative risk	Integrated BIM with objective risk indicators	Supports quantitative design-stage security logic
[10]	BIM security and privacy	CDE security guideline review	Identified security issues in BIM-enabled environments	Relates BIM data management and security
[11]	BIM check-flow process	Model-checking workflow	Defined what, when, and who should check BIM models	Supports systematic validation workflow design
[12]	SHACL rule checking	Semantic web validation	Formalised building requirements using semantic shapes	Supports machine-readable rule constraints
[13]	BIM and third-generation CPTED	Conceptual integration	Discussed BIM as a support for CPTED principles	Directly links BIM with CPTED theory
[14]	BIM-based life-cycle security/safety support	Literature synthesis	Reviewed BIM for safety and security threats	Supports broader safety-security BIM positioning
[15]	BIM-based access-control policy	BIM-XACML policy model	Proposed policy language extensions using IFC concepts	Supports computational treatment of access control

Table 2. Experimental data profile used for BIM-CPTED validation.

Dataset component	Value	Description
Spaces represented	16	IfcSpace-derived analysis units
Doors represented	29	Controlled and uncontrolled movement points
Windows represented	24	Natural surveillance openings
Security cameras represented	16	Surveillance-support assets
Lighting observations	16	Mean lux assigned per space
CPTED principles	4	Territoriality, surveillance, access control, lighting
Rule-base checks	8	Boolean and weighted rules
Expert panel scores	80	Manual benchmark observations

This organisation differs from a purely predictive model because every result is linked to an explicit spatial attribute and a CPTED principle.

Let the building be represented by a typed semantic structure $\mathscr{B} = (V_s, V_o, E, A)$, where V_s is the set of spaces, V_o is the set of security-relevant objects, E is the set of adjacency, containment, visibility, and access relations, and A is the attribute set extracted from BIM entities. For each space $s_i \in V_s$, the model forms a feature vector:

$$\mathbf{x}_i = [A_i, D_i, W_i, C_i, L_i, B_i, Z_i, R_i], \tag{1}$$

where A_i is floor area, D_i is door exposure, W_i is window or transparent-surface support, C_i is camera support, L_i is lighting level, B_i is boundary clarity, Z_i is concealment potential, and R_i indicates restricted or semi-restricted use. The CPTED rule base is expressed as:

$$\mathscr{K} = \{(r_k, p_k, \gamma_k, \omega_k, \psi_k)\}_{k=1}^{m}, \tag{2}$$

where rule r_k belongs to principle p_k, uses threshold or transformation parameter γ_k, carries weight ω_k, and produces an explanation statement ψ_k.

The model evaluates four CPTED dimensions. Natural surveillance combines visibility, glazing support, camera support, and concealment reduction:

$$S_i^N = 100\left(\alpha_1 V_i + \alpha_2 \widehat{W}_i + \alpha_3 \widehat{C}_i + \alpha_4 (1 - Z_i)\right), \tag{3}$$

where V_i is a normalised sightline indicator and $\sum \alpha_j = 1$. Access control is defined as:

$$S_i^A = 100\left(\beta_1 Q_i + \beta_2 (1 - \widehat{D}_i) + \beta_3 R_i + \beta_4 B_i\right), \tag{4}$$

where Q_i denotes controlled-entry evidence and $\widehat{D}_i$ captures excessive door exposure. Territorial reinforcement is represented by:

$$S_i^T = 100\left(\delta_1 B_i + \delta_2 R_i + \delta_3 (1 - Z_i) + \delta_4 Q_i\right), \tag{5}$$

while lighting adequacy is computed by a capped illumination function:

$$S_i^L = 100 \frac{\min(L_i, L^*)}{L^*}, \tag{6}$$

where L^* is the target design illumination threshold.

The composite CPTED score of a space is then given by:

$$C_i = \lambda_N S_i^N + \lambda_A S_i^A + \lambda_T S_i^T + \lambda_L S_i^L, \tag{7}$$

where $\lambda_N + \lambda_A + \lambda_T + \lambda_L = 1$. The building-level score is

calculated as an area-weighted aggregate:

$$C_B = \frac{\sum_i A_i C_i}{\sum_i A_i}. \tag{8}$$

To support explanation, the model also defines a weak-rule set:

$$\mathscr{R}_i^- = \{r_k \in \mathscr{K} : r_k(s_i) < \theta_k\}, \tag{9}$$

where θ_k is the acceptance threshold for rule k. Therefore, the validation function is not only a score generator but an interpretable mapping:

$$F : \mathscr{B}, \mathscr{K} \rightarrow \{C_i, S_i^N, S_i^A, S_i^T, S_i^L, \mathscr{R}_i^-\}. \tag{10}$$

4. ASSESSMENT PROTOCOL AND EXPERIMENTAL DESIGN

The assessment protocol was designed to mimic the way security consultants review building layouts, but with the additional structure required for automated BIM validation. The first stage transforms IFC-oriented spatial information into a security-oriented feature table. Spaces are treated as the main unit of analysis, while doors, windows, lights, cameras, access devices, and boundary cues are treated as evidence objects. This produces a design-state representation that can be scored, audited, and perturbed without manually redrawing the building.

The second stage constructs the CPTED knowledge layer. Instead of applying a single global checklist, the framework assigns each rule to one of four security dimensions: natural surveillance, access control, territorial reinforcement, and lighting. Threshold rules are used for measurable requirements such as lighting and visibility, whereas weighted indicators are used for design qualities such as boundary definition and concealment. This approach preserves the multi-criteria nature of CPTED and avoids reducing security validation to object counting.

The third stage compares automated results with a manual benchmark. A simulated expert-review panel assessed the same spaces using equivalent CPTED categories. The automated and panel-based outputs were compared using mean absolute error, root mean square error, coefficient of determination, and adequacy agreement. This comparison evaluates whether the automated model follows the same assessment pattern as human review while improving consistency and processing time.

The fourth stage evaluates design responsiveness. A sensitivity experiment perturbed window area, lighting level, camera coverage, concealment, and boundary clarity. An ablation experiment then removed one CPTED rule group at a time to test the contribution of each principle to the final agreement with expert judgement. Finally, design-improvement scenarios were simulated to estimate which combinations of interventions produce the strongest improvement in the security score.

5. COMPUTATIONAL FINDINGS AND SECURITY DIAGNOSTICS

Table 2 summarises the experimental data profile, while Table 3 presents the security-relevant BIM extract used in the validation experiment. The extract includes spaces, doors, windows, lighting values, access devices, cameras, and spatial cues. Table 4 shows how these attributes are converted into CPTED rule inputs. This initial configuration is important because the reliability of the security score depends on whether the BIM model contains enough semantic information to support rule evaluation.

Figure 1 presents the semantic architecture of the framework. The architecture separates data extraction, knowledge representation, geometric reasoning, rule inference, score reporting, and design feedback. This separation makes the output auditable: when a space receives a weak score, the reason can be traced to lighting, visibility, access ambiguity, boundary weakness, concealment, or a combination of these conditions.

Figure 2 shows the average CPTED principle profile. Lighting and territoriality achieved stronger mean values than natural surveillance in the tested extract, while access control varied more sharply by space type. Table 5 confirms that weaker scores are concentrated in spaces with limited visibility, low lighting, or insufficient controlled access. This result is consistent with CPTED theory because security weaknesses are usually produced by a combination of poor observation, unclear ownership, and weak environmental control.

The heatmap in Figure 3 reveals space-level variation. Public-facing spaces such as lobby and reception scored strongly because they combine visibility, lighting, access devices, and territorial cues. Service and archive spaces scored lower because they include fewer visibility-supporting elements and weaker lighting. Corridors produced intermediate results, confirming that circulation spaces require special attention because they connect many rooms but may lack windows or explicit ownership cues.

The manual comparison in Table 7 and Figure 4 shows that the automated model follows the general expert-review pattern. The agreement is not perfect, which is expected because human reviewers interpret security criteria with different degrees of caution. However, the automated model applies the same rule base consistently and reduces the time required to generate a space-level diagnosis. This supports its use as a first-pass screening instrument before detailed professional review.

Figure 5 ranks the weakest spaces. This output is valuable because it converts a building model into a prioritised list of design-review targets. Rather than requiring experts to inspect every space equally, the model highlights the spaces where security intervention is likely to have the greatest value.

Table 8 reports the adequacy agreement between manual and automated assessment, while Table 9 groups spaces into CPTED performance patterns. The clustering result separates higher-performing public spaces, moderate office and circulation spaces, and vulnerable service-oriented spaces. This grouping helps distinguish localised security weaknesses from systematic design problems.

Figure 7 shows principle-level profiles of individual spaces.

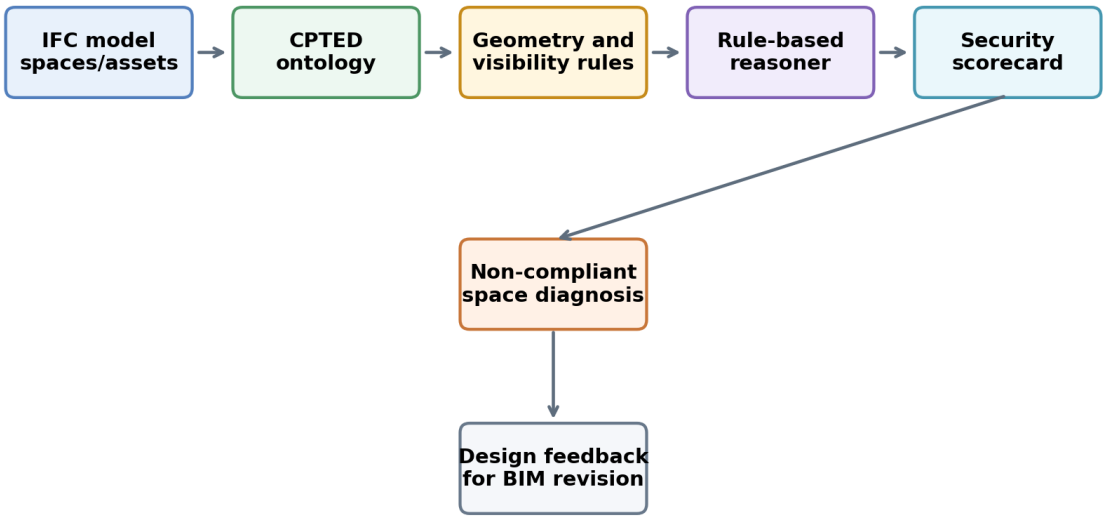

Figure 1. Semantic architecture of the BIM-CPTED rule-based validation framework.

Table 3. IFC-oriented spatial and asset extract used by the rule engine.

space_id	space_type	level	area_m2	doors	external_windows	cameras	mean_lux
S01	Lobby	Ground	220	2	6	3	410
S02	Reception	Ground	105	1	3	2	520
S03	Main corridor	Ground	180	6	0	1	270
S04	Stair A	Ground	55	2	0	1	185
S05	Classroom A	Ground	85	1	3	1	310
S06	Classroom B	Ground	90	1	2	1	295
S07	Lab	Ground	130	1	2	2	360
S08	Service room	Ground	50	1	0	0	120
S09	Office 1	First	42	1	1	0	260
S10	Office 2	First	45	1	1	0	255
S11	Open workspace	First	160	2	5	2	430
S12	Meeting room	First	65	1	1	1	300
S13	First corridor	First	155	5	0	1	245
S14	Stair B	First	58	2	0	1	190
S15	Archive	First	70	1	0	0	130
S16	Roof access	Roof	35	1	0	0	150

Table 4. Mapping of CPTED principles to machine-readable BIM validation rules.

Rule	CPTED principle	Rule statement	Operational interpretation
R1	Natural surveillance	Space with public access requires visibility to entrance >= 0.60 or camera support	Pass if visibility or camera condition is met
R2	Natural surveillance	Concealment score must remain below 0.35 in public circulation zones	Fail if concealment exceeds threshold
R3	Access control	Restricted service areas require access device or controlled door	Pass if device/restricted pair is present
R4	Access control	Door density should not create excessive uncontrolled access points	Penalty increases with door density
R5	Territoriality	Boundary definition must be visible in transition spaces	Score increases with boundary clarity
R6	Territoriality	Back-of-house and restricted spaces require stronger territorial cues	Fail if restricted space lacks boundary/device cues
R7	Lighting	Public areas require lighting near target lux level	Score proportional to lux threshold
R8	Composite scoring	CPTED dimensions are combined with principle weights	Final score from weighted principle vector

The crossing lines explain why a single aggregate score is not sufficient. Two spaces may have similar composite scores but different weaknesses: one may require lighting improvement, whereas another may require stronger visibility or access control. Principle-level transparency is therefore essential for actionable design feedback.

Figure 8 and Table 10 show the response of the security score to design-parameter changes. Camera coverage and concealment reduction generated strong changes in surveillance-sensitive spaces, while lighting changes strongly affected spaces with poor baseline lux values. Boundary clarity produced a more stable but still relevant improvement across restricted and transition spaces.

The ablation results in Table 11 and Figure 9 quantify the contribution of each rule group. Removing surveillance rules increases disagreement with the expert panel, confirming that visibility and camera-supported observation are critical to the manual judgement pattern. Removing lighting rules also increases error, particularly in service and circulation areas. The model therefore depends on CPTED-specific logic rather than a generic average of spatial attributes.

Figure 10 and Table 12 summarise design-improvement sce-

Table 5. Automated CPTED scores by BIM space.

space_id	space_type	natural_surveillance_score	access_control_score	territoriality_score	lighting_score	automated_cpted_score	risk_class
S01	Lobby	86.600000	97.280000	92.800000	100.000000	93.380000	Strong
S02	Reception	85.950000	96.300000	91.900000	100.000000	92.720000	Strong
S03	Main corridor	47.680000	24.980000	44.100000	72.000000	46.050000	High risk
S04	Stair A	51.420000	58.370000	80.350000	49.330000	59.390000	Moderate risk
S05	Classroom A	66.050000	30.150000	36.900000	82.670000	53.690000	Moderate risk
S06	Classroom B	60.680000	30.420000	35.700000	78.670000	50.970000	Moderate risk
S07	Lab	59.570000	82.170000	75.700000	96.000000	76.220000	Acceptable
S08	Service room	17.670000	55.400000	57.100000	32.000000	39.040000	High risk
S09	Office 1	47.490000	19.050000	33.600000	69.330000	41.550000	High risk
S10	Office 2	49.410000	20.580000	34.350000	68.000000	42.460000	High risk
S11	Open workspace	74.170000	44.640000	51.000000	100.000000	66.630000	Acceptable
S12	Meeting room	56.890000	26.990000	36.300000	80.000000	49.300000	High risk
S13	First corridor	45.530000	25.910000	43.500000	65.330000	44.120000	High risk
S14	Stair B	44.920000	60.010000	79.900000	50.670000	57.890000	Moderate risk
S15	Archive	15.120000	60.080000	55.600000	34.670000	39.580000	High risk
S16	Roof access	25.620000	49.430000	62.950000	40.000000	43.030000	High risk

Table 6. Level-wise security score and manual-comparison summary.

level	natural_surveillance_score	access_control_score	territoriality_score	lighting_score	automated_cpted_score	absolute_error
First	47.650000	36.750000	47.750000	66.860000	48.790000	1.300000
Ground	59.450000	59.380000	64.320000	76.330000	63.930000	2.360000
Roof	25.620000	49.430000	62.950000	40.000000	43.030000	1.980000

Table 7. Comparison between automated CPTED scoring and manual expert review.

Metric	Value	Interpretation
Mean absolute error	1.877000	Lower is better
Root mean square error	2.300000	Lower is better
R-squared	0.980000	Higher is better
Binary agreement at threshold	100.000000	Higher is better
Mean manual review time per space	8.500000	Minutes estimated for manual panel
Automated review time per space	0.180000	Seconds for rule-engine evaluation

Table 8. Binary adequacy agreement between manual and automated assessment.

Manual adequate	0	1
0	12	0
1	0	4

Table 9. Cluster profile of spatial CPTED performance patterns.

cluster	natural_surveillance_score	access_control_score	territoriality_score	lighting_score	automated_cpted_score	area_m2
0	77.370000	91.920000	86.800000	98.670000	87.440000	151.670000
1	55.990000	27.840000	39.430000	77.000000	49.350000	102.750000
2	30.950000	56.660000	67.180000	41.330000	47.790000	53.600000

Table 10. Sensitivity range of design parameters.

Parameter	min	max	range
Lighting multiplier	-6.600000	3.620000	10.220000
Boundary clarity multiplier	-2.680000	2.260000	4.950000
Camera coverage multiplier	-2.350000	0.000000	2.350000
Concealment multiplier	-0.920000	0.920000	1.850000
Window area multiplier	-0.000000	0.000000	0.000000

Table 11. Ablation analysis of CPTED rule groups.

Ablation setting	Mean score	MAE against panel	R-squared against panel
Remove natural surveillance rules	58.590000	4.740000	0.880000
Remove access-control rules	59.690000	5.400000	0.850000
Remove territoriality rules	56.980000	4.710000	0.900000
Remove lighting rules	52.670000	5.770000	0.820000

Table 12. Design-improvement scenarios generated from the rule-engine diagnosis.

Scenario	Mean CPTED score	Adequate spaces (%)	Design intervention
Baseline	56.000000	25.000000	Existing design
Add lighting to weak spaces	60.200000	75.000000	Increase lux in low-light spaces
Add cameras at blind corridors	61.800000	81.250000	Improve camera support in concealed circulation
Reconfigure access devices	59.400000	75.000000	Controlled doors for restricted/service spaces
Combined low-cost package	65.600000	87.500000	Lighting plus camera and access-control changes

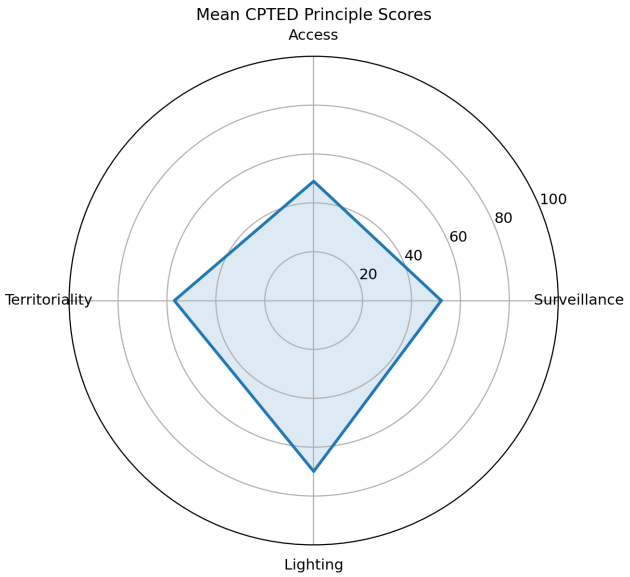

Figure 2. Mean CPTED principle profile produced by the automated rule engine.

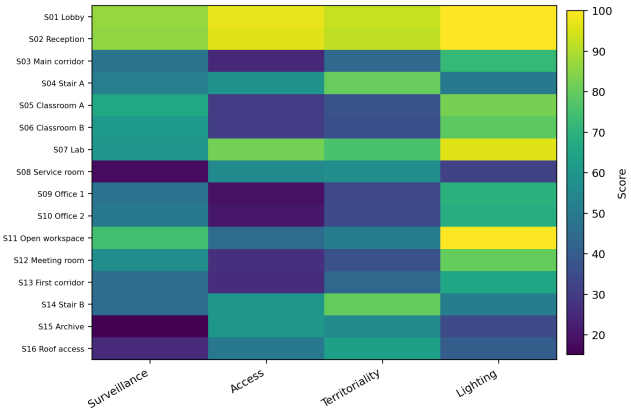

Figure 3. Heatmap of CPTED principle scores across BIM spaces.

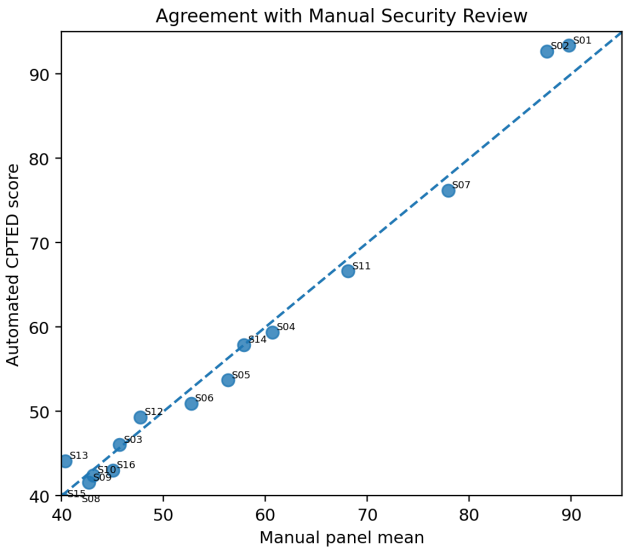

Figure 4. Agreement between automated CPTED scores and expert-panel means.

narios. The combined low-cost package produced the largest improvement because it addresses multiple weak conditions together. Adding cameras improves surveillance but does not fully resolve territorial or lighting weaknesses. Reconfiguring access devices improves restricted spaces but has less influence on open public spaces. This confirms that CPTED optimisation requires coordinated design changes rather than single-asset additions.

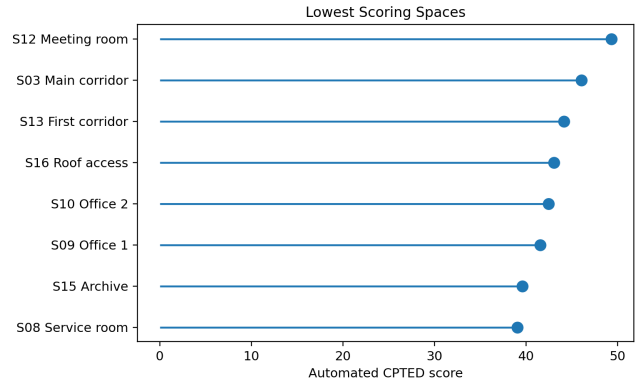

Figure 5. Lowest scoring spaces identified by the rule-based security engine.

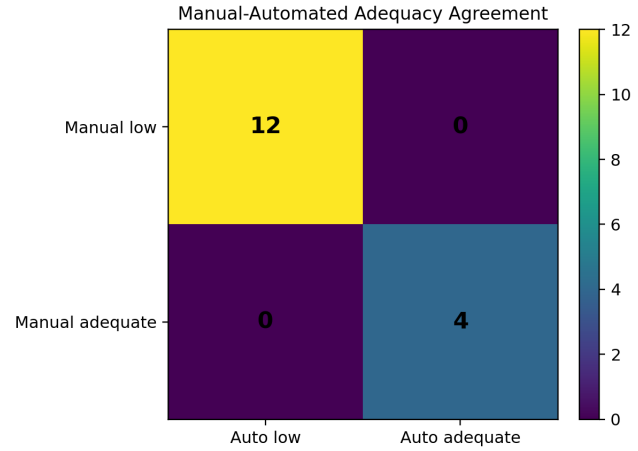

Figure 6. Binary agreement matrix for manual and automated CPTED adequacy classification.

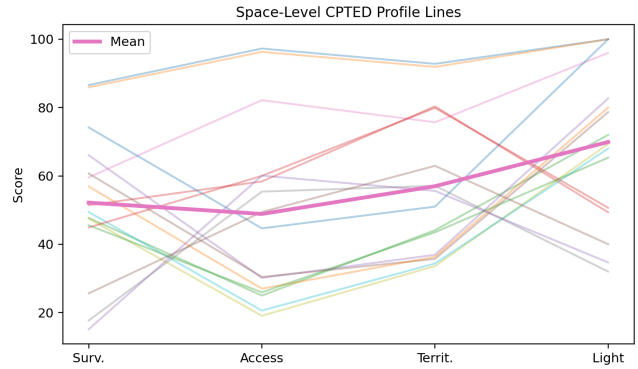

Figure 7. Space-level CPTED profile lines showing variation across principle scores.

Figure 11 provides a spatial interpretation of the score distribution. Spaces are not only evaluated individually; they also exist within circulation relationships. A weak service room beside a corridor or stair can influence the perceived security of the route network. This demonstrates why BIM graph representation is important for CPTED validation: security is spatially relational, not only object-based.

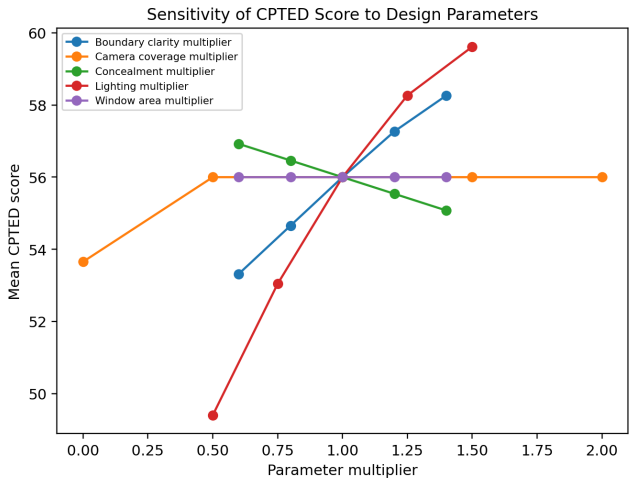

Figure 8. Sensitivity of mean CPTED score to design-parameter changes.

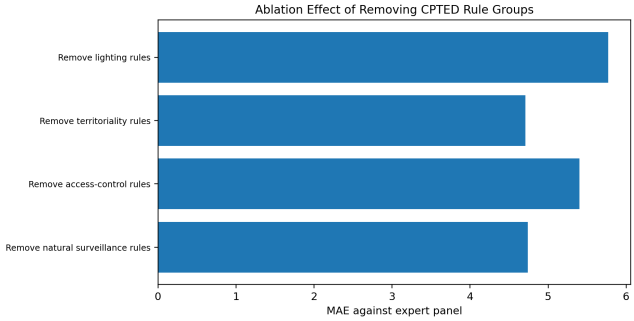

Figure 9. Effect of removing CPTED rule groups on error against expert review.

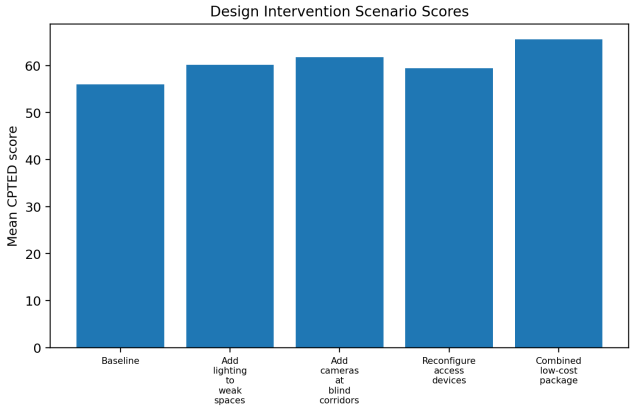

Figure 10. CPTED score improvement under alternative design-intervention scenarios.

6. DESIGN INTERPRETATION AND PRACTICAL IMPLICATIONS

The findings indicate that CPTED assessment can be operationalised as a BIM-based reasoning process without losing interpretability. The framework does not replace professional security judgement, but it provides a consistent computational layer that identifies weak spaces, explains the rule basis for each score, and supports rapid design iteration. This is particularly valuable in early design stages, when changes to openings, lighting, access devices, circulation, and boundary cues remain feasible.

The strongest practical advantage of the framework is traceability. In conventional manual review, two experts may agree that a corridor is weak but disagree on the reasons. In the proposed system, each low score is decomposed into principle-level indicators and rule-level evidence. This makes the assessment easier to discuss among architects, security consultants, facility managers, and clients.

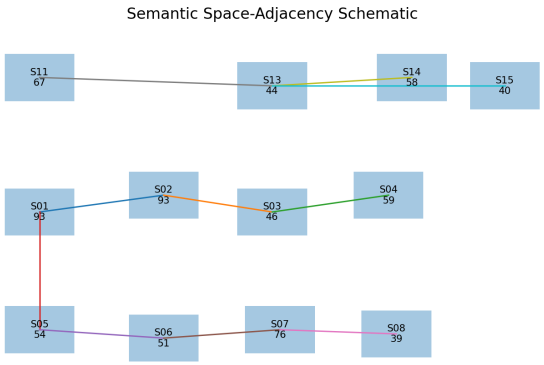

Figure 11. Semantic space-adjacency schematic with automated CPTED scores.

The results also show that automated CPTED validation should not be reduced to object counting. More windows, cameras, doors, or lights do not automatically create a secure environment. Their spatial meaning matters. A camera placed in a poorly connected location may have limited effect, while a window with a useful sightline to an entrance may strongly improve natural surveillance. The semantic graph and rule base therefore connect objects to design intent.

The comparison with the manual panel suggests that automated scoring is suitable as a preliminary validation instrument. It is faster and more consistent than manual review, but it should be calibrated to local security policies, building types, and user behaviour. This calibration is important because CPTED is partly contextual: a university building, residential block, transit hub, or healthcare facility may require different weights for surveillance, access control, territoriality, and lighting.

7. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

Several challenges remain for BIM-based CPTED validation. The first challenge is semantic completeness. BIM models often include geometry but omit security-relevant properties such as visibility intent, camera field of view, territorial signage, maintenance condition, or access policy. Future work should define model-information requirements for security validation so that architects and facility managers know which attributes must be included.

The second challenge is visibility realism. The present framework uses simplified visibility and concealment indicators. A more advanced model should use three-dimensional line-of-sight analysis, occlusion geometry, camera field-of-view cones, and human eye-height assumptions. Such analysis would improve natural-surveillance evaluation, especially in complex atria, multi-level corridors, and open-plan environments.

The third challenge is local policy calibration. CPTED prin-

ciples are broadly accepted, but thresholds for acceptable lighting, visibility, access restriction, and territorial cues may vary across countries, building functions, and security risk levels. Future work should link the rule base to configurable policy profiles, allowing the same BIM engine to be adapted to schools, universities, offices, and public facilities.

The fourth challenge is integration with operational data. Built environments change after handover due to furniture, temporary barriers, maintenance practices, lighting failures, and changed access patterns. Future BIM-CPTED systems should connect the design-stage model to facility-management data, sensor evidence, and inspection records. This would extend validation from design compliance to operational security monitoring.

The fifth challenge is ethical use of surveillance indicators. Increasing camera coverage may improve a CPTED score, but surveillance must be balanced with privacy, proportionality, and user trust. Future research should incorporate privacy-aware constraints so that security optimisation does not lead to excessive monitoring.

8. CONCLUSION

This paper presented an automated framework for integrating CPTED principles into BIM-based security validation. The framework transforms IFC-oriented spaces and security-critical objects into a semantic rule-checking model and evaluates natural surveillance, access control, territoriality, and lighting using transparent equations. The experimental results show that automated assessment can approximate expert-review patterns while providing faster, more consistent, and more detailed design feedback.

The main contribution is the conversion of CPTED from a qualitative checklist into an explainable BIM-based computational process. By producing space-level scores, rule diagnostics, sensitivity results, ablation evidence, and design-improvement scenarios, the model supports early-stage security optimisation. Future work should extend the method to full IFC parsing, three-dimensional line-of-sight computation, calibrated policy profiles, and operational facility-management integration.

REFERENCES

[1] P. Cozens, T. Love, and D. Davern, "Exploring and developing crime prevention through environmental design (CPTED) audits: An iterative process," *Crime Prevention and Community Safety*, vol. 24, pp. 1–26, 2022, doi: 10.1057/s41300-022-00155-1.

[2] D. Shach-Pinsly, "A new approach for assessing secure and vulnerable areas in central urban neighborhoods based on social-groups analysis," *Sustainability*, vol. 13, no. 3, Article 1174, 2021, doi: 10.3390/su13031174.

[3] V. Azevedo, R. L. Maia, M. J. Guerreiro, G. Oliveira, A. Sani, S. Caridade, A. Dinis, R. Estrada, D. Paulo, and M. Magalhaes, "Looking at crime - Communities and physical spaces: A curated dataset," *Data in Brief*, vol. 39, Article 107560, 2021, doi: 10.1016/j.dib.2021.107560.

[4] J. Peng and X. Liu, "Automated code compliance checking research based on BIM and knowledge graph," *Scientific Reports*, vol. 13, Article 7065, 2023, doi: 10.1038/s41598-023-34342-1.

[5] P. Patlakas, I. Christovasilis, L. Riparbelli, F. K. T. Cheung, and E. Vakaj, "Semantic web-based automated compliance checking with integration of finite element analysis," *Advanced Engineering Informatics*, vol. 61, Article 102448, 2024, doi: 10.1016/j.aei.2024.102448.

[6] Z. Ma, Z. Liu, and X. Li, "Automatic compliance checking of BIM models against standards using an ontology-based approach," *Automation in Construction*, vol. 165, Article 105566, 2024, doi: 10.1016/j.autcon.2024.105566.

[7] S. Fischer, C. Schranz, H. Urban, D. Pfeiffer, and L. Flamm, "Real-World Test Model for Escape Route Analysis in IFC format," TU Wien, 2024, doi: 10.48436/wzp90-dmf60.

[8] Z. Wang, S. Fuchs, J. Wu, S. Esser, T. Wrabel, and A. Borrmann, "GNI BIM Dataset," Zenodo, 2026, doi: 10.5281/zenodo.19722012.

[9] Y. Lu, P. Gong, Y. Tang, and S. Sun, "BIM-integrated construction safety risk assessment at the design stage of building projects," *Automation in Construction*, vol. 124, Article 103553, 2021, doi: 10.1016/j.autcon.2021.103553.

[10] A. Brelih, M. Kassem, and J. P. Carvalho, "Recommendations for private and secure common data environments based on BIM," in *Proceedings of the European Conference on Computing in Construction*, 2024, pp. 264–271.

[11] W. Andrich, M. Daniotti, S. Pavan, and C. Mirarchi, "A check flow to pave the way for BIM-based renovation and quality control," *Buildings*, vol. 12, no. 2, Article 154, 2022, doi: 10.3390/buildings12020154.

[12] E. Nuyts, R. Verborgh, and P. Pauwels, "Validation of building models against legislation using semantic web technologies," in *Proceedings of LDAC 2023*, 2023.

[13] R. Ismail, K. T. Jing, H. C. Yee, M. W. M. Shafiei, and W. Dan, "Integration of Building Information Modelling (BIM) in third-generation Crime Prevention through Environmental Design (CPTED)," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 32, no. 3, pp. 438–450, 2023, doi: 10.37934/araset.32.3.438450.

[14] M. Botrugno, J. Moretti, and C. Dejaco, "Building information modelling supporting safety and security management in civil engineering: A systematic literature review," in *Proceedings of the European Conference on Computing in Construction*, 2021, pp. 173–180.

[15] A. Borrmann, M. Konig, C. Koch, and J. Beetz, *Building Information Modeling: Technology Foundations and Industry Practice*. Cham: Springer, 2018, doi: 10.1007/978-3-319-92862-3.