*Journal of Infrastructure, Policy and Development* 2024, 8(9), 5297.
https://doi.org/10.24294/jipd.v8i9.5297

Article

# HIBLISS framework: Security & happiness by design

**Chun-lin Liu**[1,2]

[1] K&C Protective Technologies Pte Ltd, Singapore 311125, Singapore; chunlin.liu1991@gmail.com, liu.chun.lin@kcpt.com.sg
[2] AIS Communications Pte Ltd, Singapore 311125, Singapore

**CITATION**

Liu CL. (2024). HIBLISS framework: Security & happiness by design. Journal of Infrastructure, Policy and Development. 8(9): 5297. https://doi.org/10.24294/jipd.v8i9.5297

**ARTICLE INFO**

Received: 18 March 2024
Accepted: 2 July 2024
Available online: 11 September 2024



**Abstract:** Complex security systems are designed to elevate physical security. Besides people's first-hand experience of being secured, there is a secondary sensation of anxiety while being watched which should be given a particular emphasis. In this paper, first the Security & Happiness by Design Framework is proposed which is based on research findings in psychology. After a brief literature review on scholarly works addressing the intersection between security and psychology. The concept presented by HIBLISS, the Happiness Initiated Behaviour Led Intelligence Security System, underscores the integration of user well-being, behavioral analysis, and advanced technology within security frameworks. Specifically, the case study of the Jewel Airport in Singapore is cited to enhance the concept's applicability, detailing its advantages and its role in a holistic risk assessment methodology.

**Keywords:** security and happiness by design; connect-sense-response; security system; detection; infrastructure; security risk assessment; threat; terrorist attack

## 1. Introduction

### 1.1. Why is this research being undertaken?

Historically, security measures are established to enhance the physical security of citizens who use these concerned facilities or buildings. Besides the relief of this elevated level of security, a less reassured feeling emerges within people when living in a space controlled by a multisensory system. Based upon two decades of professional experience with clients, K&C Protective Technologies Pte Ltd argues that this anxiety in people should be taken into consideration when designing the security of a building. Accordingly, it is advisable that people's happiness becomes a significant factor in the planning process. Notwithstanding, applying this happiness element would considerably increase the sustainable index of a city through high social equity. Moreover, in the long run this concept could not only meet the social requirements but would result in an increased commercial demand.

The ultimate goal of security system design is asset protection by design. The term refers to "the process that allows clients to control the access that people (internal and external) have to the organization's assets" (Kelling and Coles, 1997). "Security in these concepts is guaranteed by implementing layers of business security that are tailored to the value of the assets, ensuring flexibility, efficiency, and cost-effectiveness." (Liu and Gunaratna, 2021).

The Artificial Intelligence and Machine Learning (AIML) applications include security systems. Video surveillance, by processing images of people, has proved effective and is increasingly used in both public and private domains to prevent and record crimes (Dambalkar et al., 2020). However, video surveillance recordings may also interfere with the legally protected privacy of individuals because video

surveillance records may involve processing of personal data (Cavallaro, 2007). Besides the observation and recording of images, security systems need to consider "their transmission in networks, analysis, storage and archiving of storage devices, and destruction of the recordings or the entire storage device" (Socha and Kogut, 2020). Public spaces in the city of Katowice serve as an excellent case study where smart video surveillance and analysis systems were installed with the purpose of improving security (Socha and Kogut, 2020). This project became known as Katowice Intelligent Monitoring and Analysis System (KISMiA) and the system is also designed to be scalable for future expansion where more districts can be connected to the monitoring centre for security related data to be collected within a common data environment. With a single source of truth, AIML can be better optimised, thus allowing effective coordination between the monitoring operators and the city services for a higher level of security to be achieved.

Psychology explores the mind and behavior. In the context of modern security systems, it's essential to understand that they operate as Cyber-Physical Systems (CPS), which involves the integration of computation, networking, and physical processes. (Sowe et al., 2016). Putting humans (people) in this loop defines a new discipline of CPS called Cyber-Physical Human Systems (CPHS)" or Human-in-the-Loop (Sowe et al., 2016). Engineering psychologists examine how human factors interact with machines and technology (Carayon, 2006). The principles of psychological science can be applied, which can provide guidance through the design of products, systems, and devices people use on a daily basis. The focus of these analyses lies on performance and safety. For our research, it is more relevant to scrutinize how human factors may affect the adoption of novel technologies. We need to turn to the concept of psychological acceptance that is "the active embracing of subjective experience, particularly distressing experiences" (Barnes-Holmes et al., 2001). These practices encompass various techniques such as mindfulness, cognitive distancing or diffusion, metacognition, experiential or psychological acceptance, psychological flexibility, and meditation. (Barnes-Holmes et al., 2001).

Different from the existing work, we address the problem by incorporating so-called happiness elements in the design of security systems. The development of security systems and psychology are two disconnected research areas but, undisputedly, interconnected. This research argues that much can be achieved by combining security and happiness together.

## 1.2. Theoretical foundation for the concept

### 1.2.1. The security by design concept

Arguably, the diversity and complexity of threat factors requires a thorough understanding prior to creating the plan of a building (Masys, 2018). Security by design integrates policies and measures that, when implemented, are intended to create a situation with specific desired characteristics, without causing unforeseen and undesired side effects or aftereffects. (Churchman et al., 2007). The term refers to the security architectural approach in which architects take into consideration the security needs of the concerned facility prior to its building and embed these needs in the subsequent design and construction (Bygrav, 2022). It presumes the involvement of

"an in-depth understanding of proactive security behaviour and the factors affecting it" (Arizon-Peretz et al., 2022). This concept "aims to deal with security concerns from the early phases of the system development" (Salnitri et al., 2018). Moreover, this concept offers theoretical assurances that the system in question adheres to the specified processes and security policies (Salnitri et al., 2018).

### 1.2.2. Literature review on the state-of-art on considerations where security and psychology intersect

Scholarly works have already delved into some aspects of the intersection between security and psychology. Evans' (2003) research was built upon the assertion that built environment has direct and indirect effects on mental health. The paper argued that "indirectly, the physical environment may influence mental health by altering psychosocial processes with known mental health sequelae" (Evans, 2003). More specifically, Bar-Tal and Jacobson (2007) investigated security problems through the lenses of psychology. They asserted that "security beliefs are formed based on the perception of threats in the environment, which individuals perceive as challenging to cope with." (Bar-Tal and Jacobson, 2007). Similarly, Srinivasan et al.'s work (2011) suggests that physical and mental issues correlate with built environment. Due to its public health relevance, factors within the built environment should be further examined. Based upon the authors' analysis, they recommend a "community-based, multilevel, interdisciplinary approach" to better understand the complex influence of built environment on human health (Srinivasan et al., 2011). Similarly, Tabatabaian and Tamannaee's (2014) article explored the psychological comprehension of human behavior concerning the physical environment. They concluded that "if the existing theories in environmental psychology and environmental design are applied and considered by designers, they would enhance human physical and mental health." (Tabatabaian and Tamannaee, 2014).

For livable built environments the role of these facilities in subjective well-being (SWB) is essential. Therefore, Mouratidis (2018) argues that analyzing the different perspectives on SWB is a powerful tool when planning and designing a building or when evaluating the social sustainability of planning policies. In line with this, Kumar and Mani (2019) propose a new design framework that aims to assist designers in planning sustainable smart building environment considering psychosocial aspects and mental well-being. Importantly, Altomonte et al. (2020) remember that "promoting the well-being of people is essential to achieve a more sustainable future". This necessary concept shift should take into account the advancement of "positive outcomes and the simultaneous consideration of environmental performance, human preference, and experience." (Altomonte et al., 2020). Meanwhile Hu (2020) arrived at the conclusion that certain conditions of built environment "affect human health from numerous perspectives and across multiple dimensions". More specifically, she investigated the influential factor to human health of four main categories, namely physical, physiological, biological, and psychological factors.

Visvizi and Lytras (2020) offered a widespread overview of developments in the topic of sustainable smart cities and smart villages research, including rethinking security, safety, well-being, and happiness. The authors of this special issue emphasized that "well-being and happiness must be considered as core issues in any

smart city development plan" (Visvizi and Lytras, 2020). In another research, Mouratidis (2021) takes account of seven potential pathways on how subjective well-being can be improved through urban planning. Considering the relevance of this research, for instance, he suggests to "develop or steer technology and emerging mobility options to improve inclusiveness and quality of life for different groups, integrate various forms of urban nature as much as possible, provide accessible, inclusive public spaces and communal spaces and develop aesthetically pleasing buildings and public spaces based on residents' needs and preferences" (Mouratidis, 2021). A year later, with the principles of the critical theory of security, Ardakani (2022) reconceptualized the requirements of today's security policy based upon people's happiness. At the same time, Solymosi et al.'s research (2022) aimed to draw the attention to "perceived security—the extent to which people interpret a particular situation as secure or insecure".

#### 1.2.3. Creating the definition of security and happiness by design

To address all these problems, we propose 'Security and Happiness by Design', a new concept for design and development of security systems that is based on research findings in Psychology. The Happiness Initiated Behaviour Led Intelligence Security System (HIBLISS) is a new prototype of a security system. HIBLISS is designed and implemented by combining security functionality and happiness elements of people as the priority elements. Based on our knowledge, this framework and concept are the first in the world to be applied in the field of security systems.

Based upon Hebditch's concept (2010) the following definition is proposed:

Security and Happiness by Design is identified as a concept that seeks to integrate happiness elements with the complexity of physical safety and protection into the holistic design concept of a facility, starting from the planning stage through the construction and operation phases.

The outline of this paper is as follows. First, happiness elements within security systems and the connect-sense-response principle are defined. Second, technical details of the design and implementation of HIBLISS, the Happiness Initiated Behaviour Led Intelligence Security System is detailed. Additionally, the case study of the Jewel Airport in Singapore is explained. Third, to substantiate the applicability of the concept, its advantages and its role in the holistic risk assessment methodology are presented.

## 2. Methodology for happiness index assessment systems—Introducing the concept of the HIBLISS framework

First, the happiness elements within security systems and the connect-sense-response principle will be defined. Second, technical details of design and implementation of HIBLISS, the Happiness Initiated Behaviour Led Intelligence Security System will be provided.

### 2.1. Happiness elements and connect-sense-response principle.

In our proposed security and Happiness by Design concept, the key terminology is related to happiness elements which consist of three pillars, namely environment, physical safety and security, and interpersonal relating.

1) Environment: It is about ambiance and facilities. The smell, sound, lighting, space, color, activity (buzz), when optimized, these elements generate a feeling of calmness, relaxation, comfort, safety, and a sense of being in a pleasant atmosphere.
    a. Solid state facilities: including seating areas, lights (design and color), plants, walls, chairs, carpets, information screens, facilities (washrooms, restaurants, cafes, shops, Wi-Fi, computers, exhibitions, learning environment, entertainment) collectively contribute to generating a feeling of calm, relaxation, excitement, comfort, safety, care, value, accessible luxury, acquisition (buy, connect online and a sense of being in a dynamic, exciting, opportunity filled environment).
2) Physical Safety and Security: It is about infrastructure, equipment, systems. The safety of the building includes car parks, drive in, lobby, check in, hallways, washrooms, cafes, restaurants, shops, boarding gates, blind corners, and more. Ensures the customer and staff are safe and secure, without incident, rated highly—generates a sense of confidence in physical safety and peace of mind.
    a. Equipment: visible vs hidden surveillance equipment, digital equipment shape and design of equipment, screening and checking, use of self-service technology (for convenience)—generates a sense of safety and physically secure.
    b. Systems: security clearance protocols (digital processes, searches, checking, screening, observing, random checks), staff training, how-what-where-when-who. This generates a feeling of the airport procedures being a just and equitable process, efficient systems indicating the system is working and in control—generates a sense of personal safety, emotionally security, calmness, self-discipline, confidence in safety procedures, respect for example, the airport and security personnel.
    c. For the customer to feel a personal sense of safety and security, the airport is responsible for ensuring actual safety of infrastructure (maintenance, inspections, innovation and upgrading), quality of equipment (effectiveness and efficiency), and systems and processes as working efficiently and easing customers through these systems.
3) Interpersonal relations: It is about interaction, awareness, skill and knowledge. Interpersonal relating is a social skill that is automatic to some and not to others based on their personality. The term customer care indicates a range of qualities that combine to deliver this service. Even when there will be failures and deficits in the Environmental pillar or Physical Safety and Security pillar, it is finally the human interaction that makes the difference. It is the quality of interpersonal relating that can mitigate the deficits.
    a. Interaction: A well trained staff team will be—friendly, helpful, knowledgeable, smart, decisive, confident, and will guide and lead. Supporting customers to engage with digital check in and screening systems with sensitivity. These qualities which will generate a sense of trust, respect, gratitude, care, empathy, dignity and sense of security.

b. Awareness: Staff needs to be aware of the emotional state of the customer (empathize and solve problems), cognizant of the need to process the customer through to boarding the flight (responsibility and guidance), conscious of deviance (attempts to distract and divert from security concerns), alert to safety and security concerns (safety of customer and others), and report immediately (verbally and follow-up in writing) to relevant unit of any suspicions (if customer or incident does not fit the picture or make sense or evokes concern)—generates a sense of care, support, safety, trust, confidence and respect.

c. Skill and knowledge: These qualities will be reflected in times of crisis and calm. The primary task is to know the uncertainty, needs and fears of the customer, be prepared and cater to alleviate these states. Experience, staff training, ongoing staff training, staff supervision and guidance, staff reviews and professional development are likely to ensure these qualities are inculcated. These skills generate a sense of personal value and worth, admiration and respect for staff and appreciation for standards and quality of service.

Behavioural intelligence is the application of human behaviour related knowledge and skill, to understand and explain current behaviour, predict, influence, change and manage behaviour. Behaviour led intelligence can be generated from the trinity of three domains, i.e., connect, sense and response as illustrated in **Figure 1**.

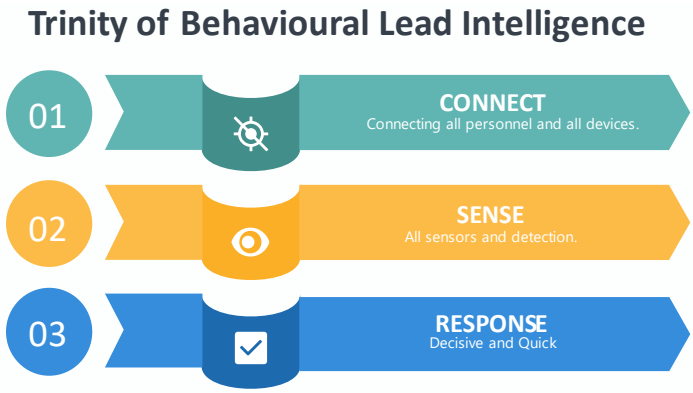



**Figure 1.** CONNECT—SENSE—RESPONSE, the behaviour Led Intelligence can be generated by this trinity to build the holistic security system (Liu, 2021).

1) CONNECT leads to connectivity and engagement between people and devices. Connectivity offers individuals a seamless means to connect with their environment and their loved ones without encountering any obstacles. They should have easy access to all the information necessary for navigating their surroundings, effectively. The ultimate outcome is information, which can be translated to security intelligence. As an illustration, when an individual exclusively communicates with family and friends from a specific location or particular flights, it may suggest a lower security alert level compared to interacting with individuals of diverse nationalities from various locations and airlines, which could warrant heightened security measures. The environment and context need to provide the individual with all the information needed for

one's consumption. The platform and the information it provides should be easily accessible to prevent frustration for both individuals and groups At the infrastructure level, ensuring connectivity for all devices is crucial. Collecting information allows for the establishment of norms and trends, facilitating the detection of changes. This adherence to connectivity enables the detection of anomalies, prompting backend monitoring systems to raise alerts. This encapsulates the fundamental principle of CONNECT.

2) SENSE involves processing the vast amount of data and information obtained from various devices and sensors, transitioning to the next domain. Through pervasive sensors constantly generating data, coupled with video analytics empowered by artificial intelligence, security personnel can proactively detect trouble or potential threats even before they manifest. The sensors will gather data and analytics to recognize patterns that could indicate if someone appears lost, emotionally distraught, or stressed. All these observations can be conducted remotely using the system outlined in this paper. Though the sensors deployed are pervasive, they need not be intrusive. The presence of sensors may be seen, yet not intimidating. These indicators only become visually apparent when necessary. By bolstering our capacity to detect subtle changes across various domains, we can effectively empower and guide individuals to feel at ease, ensuring their safety and enabling them to carry out their tasks calmly. Video analytics can also periodically monitor the "Happiness" level by detecting happy and smiling faces. Simultaneously, the system can identify abnormal behavior, unnatural or aggressive gestures, as well as strange or unusual activities and movements of people. Sensors can help to sense change there by alerting and triggering the need for a security response resulting in rapidly dispatching security without raising too much attention. The sensors that provide this data will help mitigate risk or disrupt potential incidents. In this domain of sensory processing, there are also opportunities to incorporate visual, auditory, and olfactory technologies to leverage the senses of sight, sound, and smell in inducing calmness and reducing aggression in individuals. Various therapies and techniques utilizing these sensory modalities have been supported by numerous studies.

3) RESPONSE With technology, such as smart devices and smart robotics, any potential incident can draw a rapid response within any geolocation. The system can dispatch the nearest responder or entity to aid or check on the individual in distress or under suspicion. For example, an individual may be in distress, may have dropped belongings, not able to find their way, walking back and forth, once detected, the response in the form of assistance either physically or with the use of robots could immediately be dispatched to help this person. In case of a potential argument or displays of aggressive behavior between individuals, the security personnel on a Personal Mobility Device can be promptly deployed to intervene politely. In addition to physical response, it's essential to establish a People, Processes, and Procedures Response Framework (PPPRF) to train all premises staff to be security-sensitive, enabling them to identify, respond to, and mitigate potential risks effectively. At the system level, there will be AI initiated prediction taking in the vast data from the premises like airport etc. For instance,

in an airport setting, AI could assist in forecasting the number of daily flights, analyzing flight manifests and passenger counts, predicting passenger movement patterns, identifying potential congestion at baggage claim areas, estimating dwell times within the airport, and more. Through the utilization of big data analytics powered by AI, airport operations can maintain efficiency and effectiveness, thereby reducing tension and stress for travellers.

## 2.2. The HIBLISS framework

### 2.2.1. Addressing the current security industry gap

The heightened level of security consciousness has spurred the development of novel technological innovations based on artificial intelligence (AI) aimed at mitigating security risks. However, in reality, this has not resulted in a decrease in crime but rather an increase in anxiety related to security measures. The lack of visible impact begs the question as to whether a fresh comprehensive security approach is needed. This paper attempts to address the gap. The people's need to feel safe and secure, but not watched; criminal's need to go undetected and be a step ahead of security. HIBLISS is about providing people that happiness element while ensuring maximum security.

The rapid increase in urbanisation has resulted in nearly half the world's population (55.3%) living in cities. The world's happiness ratings are largely based on assessing the subjective wellbeing of individuals in urban areas based upon evaluating factors such as congestion (transport), pollution (air), safety and stability (crime and conflict) and emotional wellbeing (sad, anxious, worry, anger) (De Neve and Krekel, 2020). Other aspects that contribute to the Happiness Index is life expectancy and future life (thriving, struggling, suffering) (Gallup, 2021). Maslow's hierarchy of needs and global happiness indexes emphasise the importance emotional well-being while being able to live within a safe, secure, and stable environment, if people are to experience happiness and life satisfaction.

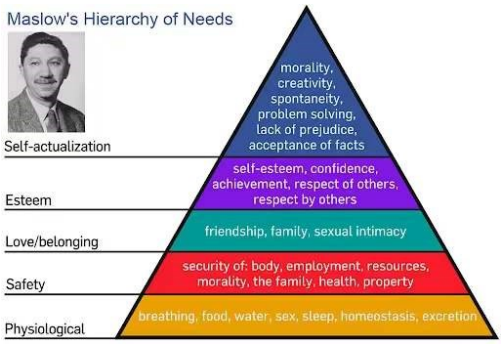



**Figure 2.** Maslow's Hierarchy of Needs (Trivedi, 2019).

Abraham Maslow's Hierarchy of Basic Needs (**Figure 2**) highlights the basic needs of people. It is the fulfilment of four basic needs, Physiological, Safety, Love/ Belongingness, and Self Esteem (deficiency factors), that allows the person to achieve the fifth level of Self Actualization (growth factor). Relevant to this paper is the Safety factor where people seek "protection from elements, security, order, law, stability, freedom from fear" (McLeod, 2007). The safety factor includes physical safety,

emotional safety and wellbeing which emphasises the need to fulfil not only the security perspective but the happiness factor, as finally it is the individual's perspective of happiness that matters within a safe and secure environment. Security measured combined with happiness elements are more likely to be accepted and appreciated than a purely security focused environment.

The paper addresses the Security & Happiness by Design, as a new concept for design and development of security systems based on research findings in psychology, incorporated into security (**Figure 3**).

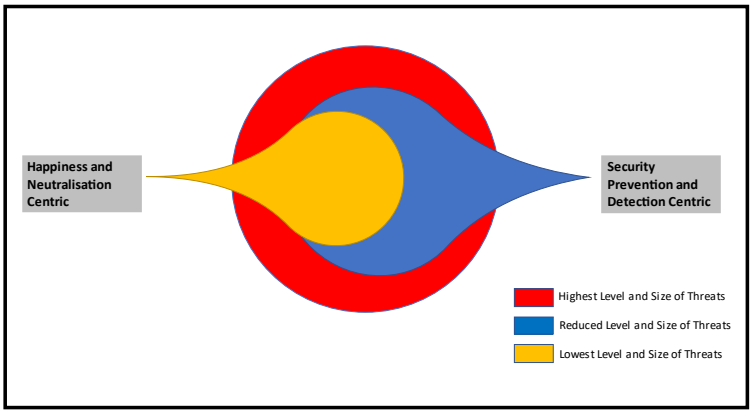



**Figure 3.** Security & Happiness by Design in Security System with Happiness Factors interwoven into Security Functions in design of the security and emergency systems (Liu, 2021).

### 2.2.2. Development and implementation of HIBLISS

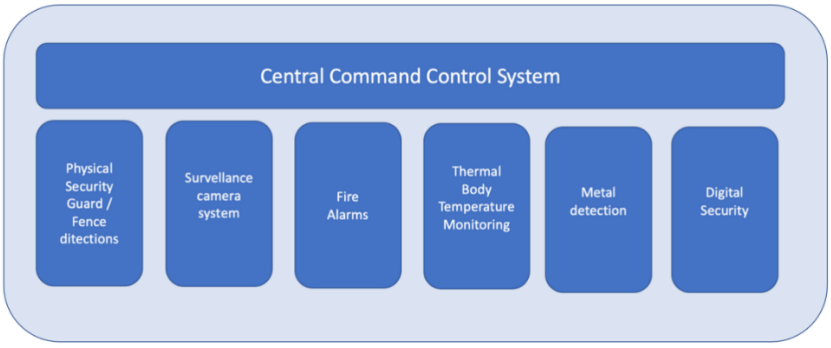



**Figure 4.** Central command control system.

Through the implementation of the new Security & Happiness by Design concept, a Happiness Initiated Behavior Led Intelligence Security System (HIBLISS) will be created through a Central Command Control Centre (**Figure 4**). HIBLISS transitions the traditional security system from a preventive and resistance-oriented approach to one focused on creating enduring happiness and resilience. This shift aims to neutralize, harmonize, and reduce the likelihood of security incidents. It instills a sense of safety, peace, and calmness in individuals within any environment, thereby reducing the motivation to engage in aggression or harm others (Liu, 2021). The technological innovations of the 4th Industrial Revolution, including 5G, data analytics, and generative artificial intelligence, provide an ideal environment for the

implementation of behavior-driven intelligence. Information holds significant power, particularly when contextualized, as it can transform into intelligence. This intelligence is derived from the extensive data collected through various channels, facilitating the analysis of behavior to generate meaningful insights. Hence forming the concept of the Happiness Initiated Behaviour Led Intelligence Security System (Liu, 2021).

**(a)** Physical security.

**(b)** Physical security.

**(c)** Fence detection system.

**(d)** Security guards.

**Figure 5.** Physical Security/Guards/Fence detection system.

Physical security with key is one of the considerations to ensuring the security to access the building premises or facilities. There are various physical security controls that can be applied such as security guards, dogs, fence detections and door access controls (**Figure 5**). However, when entering the building premises security guards verify the identity and record some personal information such as national security number, name, address, and mobile number which validate and issue the temporary access card. When the registration process records minimal amount of personal data and stored happiness rate will be medium to very high. On the other hand, the registration process collects a lot of personal information and retains it for a certain period to alert or analyse crime. While the personal data is not fully protected, experienced hackers can access the data by using technical skills, compromising privacy. Other traditional physical security controls such as dogs and traditional fence, guards ensure certain level of security while providing high level of happiness ratings of the people because they are not required to record personal data.

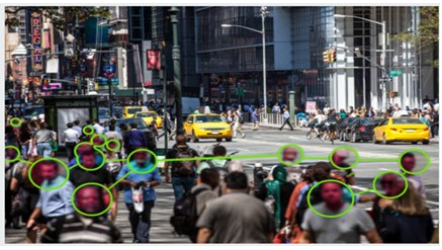
As stated above, new technologies are widely used in the security system such as facial recognition software, touchless access systems and temperature-sensing cameras which provide high-level of assurance of the security while it is embedded with Artificial Intelligence and Machine Learning (AIML) capabilities and integrated with other security platform which analyses people and activities to prevent crimes

(**Figure 6**). When privacy by design principle is applied it can result in an increased level of happiness as mentioned in **Tables 1** and **2** below.

**(a)** Incident based alert triggering software.

**(b)** Camera with AIML.

**(c)** Facial recognition camera.



**(d)** Facial recognition software.

**Figure 6.** Different types of surveillance camera systems.

Understandably, cameras blending into the surroundings—the surveillance equipment that is visible, large, square, etc., in resting areas, lobbies and seating areas will cause discomfort, hyper-alertness and privacy concerns, leading to distress and lower happiness ratings. Hence, apart from avoiding large and square cameras, the placement of the camera and ability to blend into surrounding environment are crucial for happiness-by-design adaptation.

**Figure 7.** See examples at Fulton Street Station, New York (New York Daily News, 2018).

In addition, a higher concentration of cameras, such as those at cashier counters, main entrance security screening, and security clearance areas, can negatively impact happiness (**Figure 7**). It will create an atmosphere of no space for creativity, relaxation, or enjoyment, but being alert and waiting for an incident to happen. In happiness-by-design, it should be considered to deploy only the most sufficient cameras but not in

an overwhelming quantity. Surveillance cameras installed in various places, which are expected to cover public/crowded areas, common areas such as lobbies, and special areas like blind spots, where these cameras can be focused and adjusted to cover certain degrees as per site requirements.

### 2.2.3. Use case for the HIBLISS implementation

Arguably pseudo-psychological aspects were considered with regards to one of the most notable architectural projects in Singapore. The Jewel Changi Airport in Singapore is well-known as a noteworthy shopping and entertainment complex (**Figure 8**). With a consistently high terrorist threat level, national strings on applicable security measures have always been in the forefront in the country's legislation (Liu and Gunaratna, 2022). In accordance with a 2017 modification, the security of critical national infrastructures is to be elevated by protecting their "perimeter, access points and technology infrastructure" (Ministry of Home Affairs, 2017). The security concept applied at Jewel Changi Airport in Singapore seeks to meet the interests of several perspectives. Inherently, the security system should function in a way that it disrupts the site's operation only at a minimum scale. The elevated and holistic level of security at the site should be provided in a prompt and discreet manner. The highest quality perimeter and hostile vehicle mitigation solutions were carried out. Aesthetical implementations are of great importance considering the unique architecture of the complex. In line with this, aesthetics were important factors with regards to the appearance of robust physical security elements. Additionally, installers of its security systems kept a constant eye on blending the protective infrastructure into the environment of the airport (ATG, 2018). The wellbeing and secure feeling of the users of this complex has been the primary aspect during the planning and implementation of the project.

**Figure 8.** Jewel Changi Airport, Singapore (Jenkins, 2020).

## 3. Happiness index application in the optimized security risk assessment methodology

Besides assessment criteria for artificial intelligence, considering happiness elements in the optimized security risk assessment methodology for the building under the security by design brings novel perspectives into the systematic framework of threat assessment, vulnerability assessment and consequence (impact) assessment (**Figure 9**).

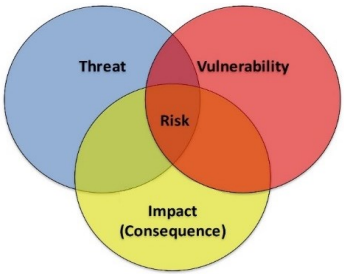



**Figure 9.** Interactive risk analytics.

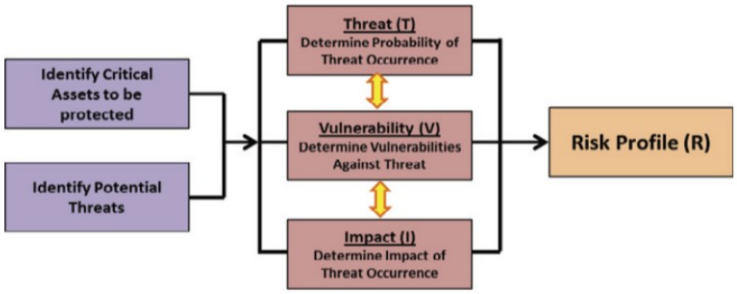



**Figure 10.** Risk assessment process.

The detailed process can be summarized as follows: 1) identify protected asset, functions, and personnel; 2) take threat assessment; 3) perform vulnerability assessment; 4) use the results from threat assessment, vulnerability assessment and impact assessment to calculate risk by (**Figure 10**).

$$R = T \times V \times I \quad (1)$$

where *R* is risk rating, *T* is threat rating, *V* is vulnerability rating, and *I* is impact rating (Liu, 2021).

### Happiness ratings

Major surveillance systems are created to observe or document the actions of either a collective or an individual, capturing data pertaining to identifiable individuals or their personal information. Therefore, surveillance systems need to ensure data protection and privacy and adhere to such data protection laws. Today, many companies use surveillance systems to monitor the entry of staff and visitors to their premises, aiming to prevent crime and illegal activities.

Happiness Ratings combine the 5-rating tables (**Tables 1–8**) as below:

**Table 1.** Privacy ratings.

| Ratings | Score | Description: Privacy Rating |
|---|---|---|
| Very high | 5 | The system will predict the crime by analysing people's real-time behaviour based on artificial intelligence. No personal data is required and stored. |
| High | 4 | The system needs to collect minimal amount of personal data and analyse the data base on Artificial intelligence. Personal data will be safely stored and destroyed after a predetermined time period. |
| Medium | 3 | The system needs to collect a moderate amount of personal information to prevent crime. While the personal data will be fully protected and safely stored. These data will be destroyed after a predetermined period of time. |
| Low | 2 | The system needs to collect a high level of personal information to alert crime. Personal data is not fully protected. An experienced hacker may be able to access the data by using technical skills. |
| Very low | 1 | The system needs to collect a high level of personal information to alert crime. Personal data is easily accessible. |

**Table 2.** Assessment criteria for privacy ratings.

| Assessment Criteria | Use Cases/Scenarios |
|---|---|
| Body capture | Install cameras to cover full body of the person(s)<br>System will cover entire body of each person and analyze the activities of the people based on Artificial intelligence when detecting suspicious activities. |
| | Install cameras to cover full body of the person(s)<br>Install cameras to cover the upper body of the person(s).<br>Cameras will configure based on the areas needed to be highly protected. |
| | Install cameras to cover upper body of the person(s)<br>System to cover upper body of each person and analyze the activities of the people based on Artificial intelligence on detecting any suspicious activities/ facial recognition, etc. |
| | Install cameras to cover the lower body of the person(s).<br>Cameras installed for special purposes/special areas to cover, for the purpose to be ensuring the privacy. |
| Data retaining period | No personal data is required or stored.<br>The system will predict crime by analyzing people's real-time behaviour based on artificial intelligence. Therefore, it is not required to store personal data. |
| | Personal data will be safely stored and destroyed after a predetermined time period (e.g., up to 3 months).<br>By default, the system collects a minimal amount of personal data and analyzes it using artificial intelligence to minimize crime.<br>Personal data to be retained for up to 3 months for further analysis if necessary.<br>After 3 months the database will be overwritten, preventing the recovery of any previous data. |
| | Personal data will be safely stored and destroyed after a predetermined time period (e.g., up to 6 months).<br>The system collects a minimal amount of personal data and analyzes it using artificial intelligence to minimize crime and assist in ongoing investigations. |

**Table 3.** Artificial intelligence ratings.

| Ratings | Score | Description: AI Rating |
|---|---|---|
| Very high | 5 | More than 50% of cameras installed for Video Surveillance Systems have Basic and Advance Video Analytic functionality. |
| High | 4 | Between 25%–50% of cameras installed for Video Surveillance Systems have Basic and Advance Video Analytic functionality. |
| Medium | 3 | Between 5%–25% of cameras installed for Video Surveillance Systems have Basic and Advance Video Analytic functionality. |
| Low | 2 | Between 1%–5% of cameras installed for Video Surveillance Systems have Basic Video Analytic functionality. |
| Very low | 1 | The Video Surveillance Systems do not have any Video Analytic functionality. |

Note: Above scales have been used since 2015 in the field of security to assess risk (KCPT).

**Table 4.** Assessment criteria for artificial intelligence ratings.

| Assessment Criteria | Use Cases/Scenarios |
|---|---|
| Operation Time | System operation time: 24/7<br>Camera System will operate 24/7 based on business operations to provide maximum security. |
| | System operation time: 6 am to 8 pm<br>Camera System will operate during business hours.<br>Alternative security will cover non-business hours (e.g., security guards) |
| | System operation time: 8 pm to 6 am<br>Camera System will be operational and activated only during this period. |
| Information Sharing | System operations by local technical team.<br>The system and database will be fully operational and managed by a local team and no third party will be involved. The service provider will be consulted only for maintenance, prescheduled services, and system upgrade. |
| | System operations by local technical team and third-party service provider.<br>Local team and service provider will operate/manage the database under the supervision of the local team. The local staff/team will hold access privileges. The service provider has no access to the data base. |
| | System operations outsourced to a third-party service provider.<br>Obtain clearance for the service provider to operate/manage the system based on the operation requirement. |

As Artificial Intelligence evolves, it has magnified the ability to use personal information in ways that can intrude on privacy interests such as the Facial recognition system. Although AI brings superior object recognition and event recognition capabilities, where it could provide proactive and real-time security with the leverage on 5G without the need of intruding on privacy-sensitive data analysis at all. Massive information can be gathered within a crowd in large spaces and Big Data analytic could extract valuable insights related to abnormal behaviour led intelligence. At the same time security and operational staff can be freed up to focus on more than just surveillance duties, where they could look at customer/stakeholders' satisfaction, what the customer/stakeholders liked the most and strive for excellent services to create happiness rating based on **Tables 1–8**.

**Table 5.** Camera concentration ratings.

| Ratings | Score | **Description: Camera concentration rating<br>(Human traffic area: Main entrances, secondary entrances and exits, lobbies and other customer areas, employee areas, counter/cash registers, seating areas, restaurant kitchens, etc. It will be measured by number of cameras per location of interest.)** |
|---|---|---|
| Very high | 5 | More than 15 cameras are needed to maintain ideal surveillance coverage. |
| High | 4 | Between 10–15 cameras are needed to maintain ideal surveillance coverage. |
| Medium | 3 | Between 5–10 cameras are needed to maintain ideal surveillance coverage. |
| Low | 2 | Between 2–5 cameras are needed to maintain ideal surveillance coverage. |
| Very low | 1 | Between 1–2 cameras are needed to maintain ideal surveillance coverage. |

**Table 6.** Assessment criteria for camera concentration ratings.

| Assessment Criteria | Use Cases/Scenarios |
|---|---|
| Location | Install cameras to cover only the exterior of the buildings, including the car park, main entrance, fence, and garbage collection point. |
| | Install cameras to cover the inside of the buildings, including the main lobby, lift lobby, and corridors. Surveillance system implemented to monitor activities outside the building and common areas. Activities of the staff, visitors, contractors, and service providers is monitored closely. |
| | Install cameras inside the buildings, including the lunchroom and restroom entrance. |
| Coverage | Install cameras with 360-degree coverage.<br>Install cameras to cover the entire area to monitor and provide maximum coverage. |
| | Install cameras with 180-degree coverage.<br>Install cameras to cover a limited area to monitor and provide coverage. |
| | Install cameras with less than 180-degree coverage.<br>Install cameras to cover a limited area to monitor and provide coverage. |

**Table 7.** Camera placement and blend into the environment ratings.

| Ratings | Score | Description: Camera placement and blend into the environment rating (Human traffic area: Main entrances, secondary entrances and exits, lobbies and other customer areas, employee areas, counter/cash registers, seating areas, restaurant kitchens, etc. It will be measured by number of cameras per location of interest.) |
|---|---|---|
| Very high | 5 | All cameras are unnoticeable and are blended into the environment. |
| High | 4 | 1%–10% of cameras are noticeable and exposed without blending into the environment. |
| Medium | 3 | 10%–50% of cameras are noticeable and exposed without blending into the environment. |
| Low | 2 | 50%–80% of cameras are noticeable and exposed without blending into the environment. |
| Very low | 1 | More than 80% of cameras are noticeable and exposed without blending into the environment. |

**Table 8.** Assessment criteria for camera placement and blend into the environment ratings.

| Assessment Criteria | Use Cases/Scenarios |
|---|---|
| Location | Install cameras to cover only outside the buildings (car park, main entrance, fence, garbage collection point). Surveillance systems are implemented to monitor activities outside the building. |
| | Install cameras to cover inside the buildings, main lobby, lift lobby, corridors. Surveillance systems are implemented to monitor activities outside the building and common areas. Activities of the staff, visitors, contractors, and service providers are monitored closely. |
| | Install cameras inside the buildings including the lunchroom, restroom entrance. |

## 4. The benefits of applying the HIBLISS framework

Incorporating happiness elements into a construction can enhance resistance to a blast incident. For instance, building double walls and adding aesthetical details (pictures, green walls, or architectural designs) will help people accept these solutions. Meanwhile, reinforced structures with these extraordinary walls substantially increase the blast resistance of the building. Another example can be the replacement of anti-crash bollards systems with planter boxes, chairs/benches, or trees. These are excellent substitutions to prevent the unauthorized access of vehicles. People tend to apply more of these aesthetic structures, that besides bringing joy to visitors, considerably harden the malevolent access to the building. Taking account of the benefits of anti-blast walls, instead of steel plates with RC wall, green walls bring the same security-related advantages, while igniting a pleasant feeling of people passing by. With regards to

transition areas in lobbies, front and back doors should be repositioned, and instead of locating them in one straight line, it is better to look at these entrances and entries placed in a curved line.

Examples illustrating the concepts of Security by Design and Security and Happiness by Design will be presented:

1) To prevent authorized vehicle against impact loading,
   (1) Anti-crash Bollard's system (Security by Design) (**Figure 11**).

**Figure 11.** Anti-crash Bollard's system.

   (2) Proposed Anti-Crash Landscape (such as planter box, chair, tree, etc.) (Security and Happiness by Design). (**Figure 12**).

**Figure 12.** Proposed Anti-Crash Landscape.

2) For anti-blast wall against blast loading.
   (1) Steel plate with RC wall (Security by Design) (**Figure 13**).


**Figure 13.** Steel plate with RC wall.

(2) Anti-Blast Green wall (Security and Happiness by Design) (**Figure 14**).

**Figure 14.** Anti-Blast green wall.

3) Transition area against blast loading.
   (1) Lobby area (door opening) (Security by Design): front door and back door in one straight line.
   (2) Lobby area (door opening) (Security and Happiness by Design) front door and back door in one curve line.

## 5. Conclusion

This paper has first, defined the happiness elements within security systems and the connect-sense-response principle. Second, technical details of design and implementation of HIBLISS, the Happiness Initiated Behaviour Led Intelligence Security System has been provided. More specifically, the case study of the Jewel airport in Singapore is cited. To substantiate the applicability of the concept, its advantages and its role in the holistic risk assessment methodology has been presented.

This research represents the first step of our project in the fields of security and psychology. An upcoming phase will include the author's work on theory and implementation and will address the proposed design and implementation. The third phase of this project will show empirically the importance of security design for psychology and the importance of how the cyber-physical security system will work in this environment. After the experimental design of this study, its results will be reported and discussed. The research will conclude with suggestions for future work.

**Conflict of interest:** The authors declare no conflict of interest.

## References

Altomonte, S., Allen, J., Bluyssen, P. M., et al. (2020). Ten questions concerning well-being in the built environment. Building and Environment, 180, 106949. https://doi.org/10.1016/j.buildenv.2020.106949

Ardakani, A. E. (2022). A theoretical review on security policy making on people's happiness. Strategic Studies Quarterly, 25(96).

Arizon-Peretz, R., Hadar, I., & Luria, G. (2022). The Importance of Security Is in the Eye of the Beholder: Cultural, Organizational, and Personal Factors Affecting the Implementation of Security by Design. IEEE Transactions on Software Engineering, 48(11), 4433–4446. https://doi.org/10.1109/tse.2021.3119721

ATG. (2018). Jewel Changi Airport. Available online: https://atgaccess.com/cases/jewel-changi-airport/ (accessed on 15 March 2024).

Barnes-Holmes, Y., Steven, C. H., Dermot, B.-H., Roche, B. (2001). Relational frame theory: a post-Skinnerian account of human language and cognition. New York: Plenum Press. https://doi.org/10.1016/S0065-2407(02)80063-5

Bar-Tal, D., & Jacobson, D. (1998). A Psychological Perspective on Security. Applied Psychology, 47(1), 59–71. Portico. https://doi.org/10.1111/j.1464-0597.1998.tb00013.x

Brown, S. R. (2018). MTA owed $667,000 from retail giant Westfield for rent at Fulton Center: suit. New York Daily News. Available online: https://www.nydailynews.com/new-york/ny-metro-mta-westfield-rent-20181219-story.html (accessed on 19 May 2021).

Bygrave, L. A. (2022). Security by Design: Aspirations and Realities in a Regulatory Context. Oslo Law Review, 8(3), 126–177. https://doi.org/10.18261/olr.8.3.2

Carayon, P. (2006). Human factors of complex sociotechnical systems. Applied Ergonomics, 37(4), 525–535. https://doi.org/10.1016/j.apergo.2006.04.011

Cavallaro, A. (2007). Privacy in Video Surveillance [In the Spotlight]. IEEE Signal Processing Magazine, 24(2), 168–166. https://doi.org/10.1109/msp.2007.323270

Churchman, C. W., Protzen J.-P., Webber M. M., Krogh, D. (2007). In Memoriam: Horst W.J. Rittel. Design Issues, 23(1), 89-91.

Dambalkar, P., Gupta, A., Pande, A., Ladekar, A. (2020). Smart Surveillance System -Literature Survey. International Research Journal of Engineering and Technology (IRJET), 7(5).

De Neve, J.-E., Krekel, C. (2020). Cities and Happiness: A Global Ranking and Analysis. Last Modified March 20, 2020. Available online: https://worldhappiness.report/ed/2020/cities-and-happiness-a-global-ranking-and-analysis (accessed on 5 May 2020).

Evans, G. W. (2003). The Built Environment and Mental Health. Journal of Urban Health: Bulletin of the New York Academy of Medicine, 80(4), 536–555. https://doi.org/10.1093/jurban/jtg063

Gallup. (2021). Understanding How Gallup Uses the Cantril Scale. Available online: https://news.gallup.com/poll/122453/understanding-gallup-uses-cantril-scale.aspx (accessed on 6 June 2021).

Greene, D., Hoffmann, A. L., & Stark, L. (2019). Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning. Proceedings of the 52nd Hawaii International Conference on System Sciences. https://doi.org/10.24251/hicss.2019.258

Hebditch David, J., Third Sinclair, J., Martin Jon, P., Wise, M. (2010). International Development of Safeguards and Security by Design of Nuclear Facilities and Processes. March 7-11. Phoenix, AZ, U.S.A. Available online: https://archivedproceedings.econference.io/wmsym/2010/pdfs/10030.pdf (accessed on 6 June 2021).

Horowitz, M. C., Gregory, C., Allen, E., et al. (2018). Artificial Intelligence and International Security. Artificial Intelligence and International Security.

Hu, M. (2020). Factors that impact human health in the built environment. In: Smart Technologies and Design For Healthy Built Environments. Springer, Cham. https://doi.org/10.1007/978-3-030-51292-7_3

Jenkins, K. (2020). The spectacular Jewel at Changi Airport. Available online: https://velvetescape.com/jewel-changi-airport/ (accessed on 15 February 2024).

Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. Defense & Security Analysis, 35(2), 147–169. https://doi.org/10.1080/14751798.2019.1600800

Kelling, G. L., Coles, C. M. (1997). Fixing Broken Windows: Restoring Order And Reducing Crime In Our Communities: Simon and Schuster. Free Press.

Kumar, T., & Mani, M. (2019). Discerning Occupant Psychosocial Behaviour in Smart Built Environment and its Design. Proceedings of the 1st ACM International Workshop on Urban Building Energy Sensing, Controls, Big Data Analysis, and Visualization. https://doi.org/10.1145/3363459.3363534

Landoll, D. (2021). The Security Risk Assessment Handbook. CRC Press. https://doi.org/10.1201/9781003090441

Liu, C.-L. (2021). Security & Happiness by Design for Happiness Initiated Behavioural Lead Intelligence Security System (HIBLISS). Civil Engineering Research Journal, 12(2). https://doi.org/10.19080/cerj.2021.12.555832

Liu, C.-L., & Gunaratna, R. (2021). Lebanon's Single Most Destructive Explosion - Terrorists Plan to Copy and Provision against Such Accidents. Journal of Applied Security Research, 1–22.

Liu, C.-L., & Gunaratna, R. (2022). Global threat landscape 2022. UNISCI Journal, 20(58), 141–144. https://doi.org/10.31439/unisci-137

Masys, A. J. (2018). Security by Design Innovative Perspectives on Complex Problems. Cham: Springer International Publishing.

McLeod, S. (2007). Maslow's Hierarchy of Needs. Available online: https://www.simplypsychology.org/maslow.html (accessed on 6 May 2020).

Ministry of Home Affairs. (2017). Infrastructure Protection Act. Available online: https://www.mha.gov.sg/what-we-do/managing-security-threats/protecting-infrastructure (accessed on 6 May 2020).

Mouratidis, K. (2018). Rethinking how built environments influence subjective well-being: a new conceptual framework. Journal of Urbanism: International Research on Placemaking and Urban Sustainability, 11(1), 24–40. https://doi.org/10.1080/17549175.2017.1310749

Mouratidis, K. (2021). Urban planning and quality of life: A review of pathways linking the built environment to subjective well-being. Cities, 115, 103229. https://doi.org/10.1016/j.cities.2021.103229

Nakagaki, T., Kobayashi, R., Nishiura, Y., et al. (2004). Obtaining multiple separate food sources: behavioural intelligence in the Physarum plasmodium. Proceedings of the Royal Society of London. Series B: Biological Sciences, 271(1554), 2305–2310. https://doi.org/10.1098/rspb.2004.2856

New York Daily News. (2018). MTA owed $667,000 from Retail Giant Westfield for Rent at Fulton Center: suit. Available online: https://www.nydailynews.com/new-york/ny-metro-mta-westfield-rent-20181219-story.html (accessed on 15 February 2024).

Salnitri, M., Alizadeh, M., Giovanella, D., et al. (2018). From Security-by-Design to the Identification of Security-Critical Deviations in Process Executions. In: Mendling, J., Mouratidis, H. (editors). Information Systems in the Big Data Era. CAiSE 2018. Lecture Notes in Business Information Processing, Volume 317. Springer, Cham. https://doi.org/10.1007/978-3-319-92901-9_19

Socha, R., & Kogut, B. (2020). Urban Video Surveillance as a Tool to Improve Security in Public Spaces. Sustainability, 12(15), 6210. https://doi.org/10.3390/su12156210

Solymosi, R., Guedes, I., Vozmediano, L. (2022). Using Mobile Applications and Physiological Sensing to Measure Perception of Security in Built Environments. In: Gill, M. (editors). The Handbook of Security. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-91735-7_26

Sowe, S. K., Simmon, E., Zettsu, K., et al. (2016). Cyber-Physical-Human Systems: Putting People in the Loop. IT Professional, 18(1), 10–13. https://doi.org/10.1109/mitp.2016.14

Srinivasan, S., O'Fallon, L. R., & Dearry, A. (2011). Creating Healthy Communities, Healthy Homes, Healthy People: Initiating a Research Agenda on the Built Environment and Public Health. American Journal of Public Health, 93(9), 1446–1450. https://doi.org/10.2105/ajph.93.9.1446

Tabatabaian, M., Tamannaee, M. (2014). Investigation the Effect of Built Environments on Psychological Health. Journal of Architecture, Urban Design and Urban Planning, 6(11)

Trivedi, A. J. (2019) Maslow's Hierarchy of Needs. A theory of human motivation. International Journal of Research in all Subjects in Multi Languages, 7(6).

Visvizi, A., & Lytras, M. D. (2020). Sustainable Smart Cities and Smart Villages Research: Rethinking Security, Safety, Well-being, and Happiness. Sustainability, 12(1), 215. https://doi.org/10.3390/su12010215