BUILDING
Cyber Security

Framework Review

www.buildingcybersecurity.org

Our Mission

Establish and sustain frameworks developed by stakeholders across multiple sectors and administered by a non-profit organization offering market-driven options to promote cyber protections in controls and devices for enhanced cyber-physical security and safety in an increasingly smart world.

Our Vision

Building Cyber Security (BCS) will be the premier global administrator certifying operational technologies, processes, training, and recovery plans for safe, secure use of controls and devices.

Framework Goals & Requirements

CORE DESIGN PRINCIPLES

- Leverage existing technical standards to avoid duplication
- Ensure framework is modular, evolving, and consistent with technology and industry changes
- Includes all building technology (OT and IT that supports/interfaces with OT)

REQUIRED OUTCOMES

- Foster a cybersecurity culture in the building industry
- Alignment of cybersecurity risk into business risk
- Stakeholder have incentive to adopted (insurance coverage)

Deliverables

1. Risk framework (with value model)
2. Industry Standard Profile
3. Certification & labeling scheme

CRE Cyber Risk Include Both OT & IT

Cyber-Physical Risk (OT)

Information Risk (IT)

OT

IT

PHYSICAL SYSTEMS

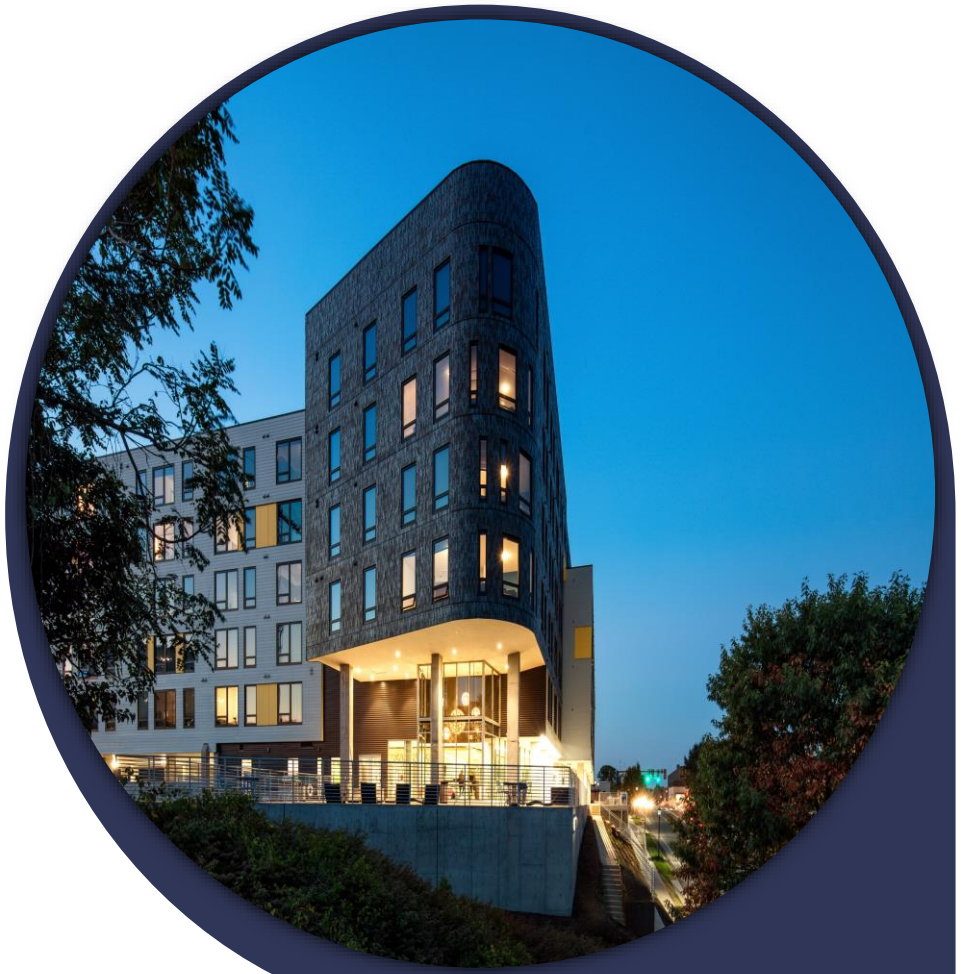
- HVAC
- Lighting
- Access Control
- Parking
- Video Surveillance

BUILDING TECHNOLOGY

- Building Management
- Building Automation
- IOT/Sensors

INFORMATION TECHNOLOGY

- Property Management
- Billing
- Work Order System

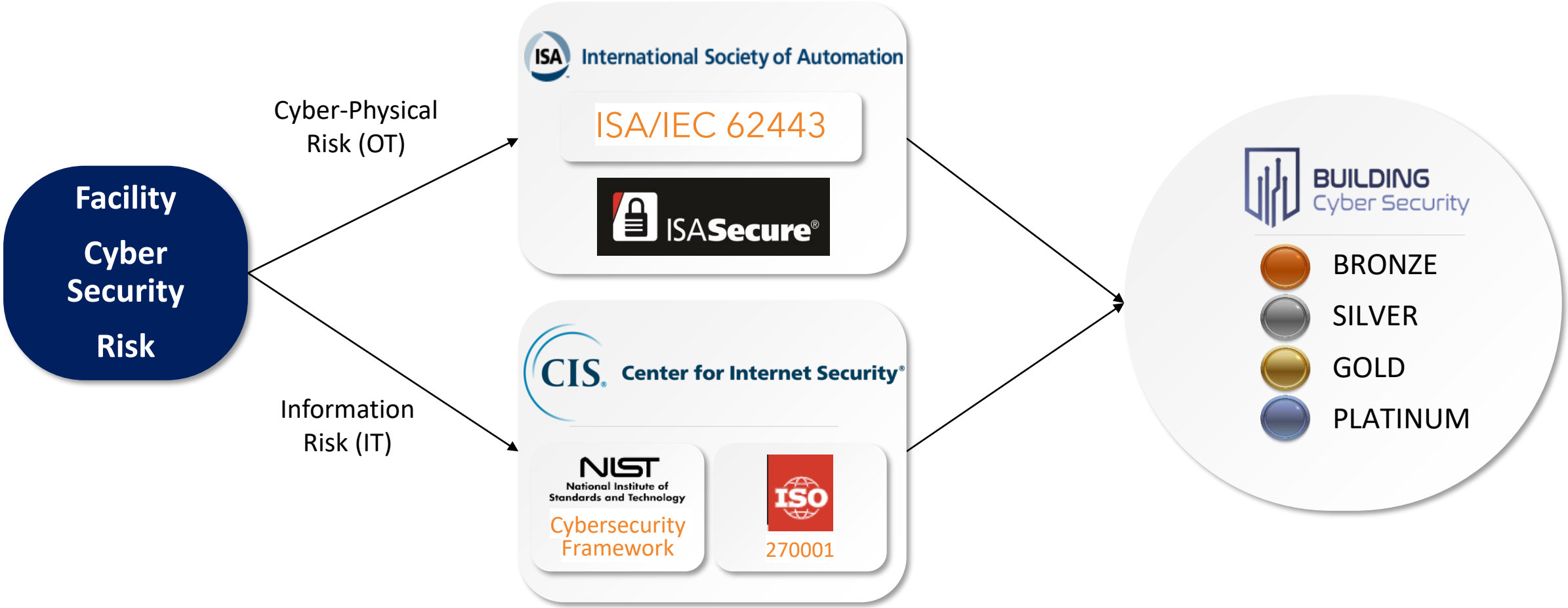


BCS Rating Schema

		Bronze	Silver	Gold	Platinum
OT Zones	Building Functional Areas (Standard Zones)	59/86	81/86	86/86	86/86
	Health Safety Environmental Areas (Essential Zones)	64/90	85/90	90/90	90/90
	Security Processes Maturity Level	Repeatable	Repeatable	Repeatable	Improving
IT Zones	CIS Controls	IG1 58/156	IG2 133/156	IG3 156/156	IG3 156/156

* Final BCS rating is based on the lowest score between OT and IT scoring.

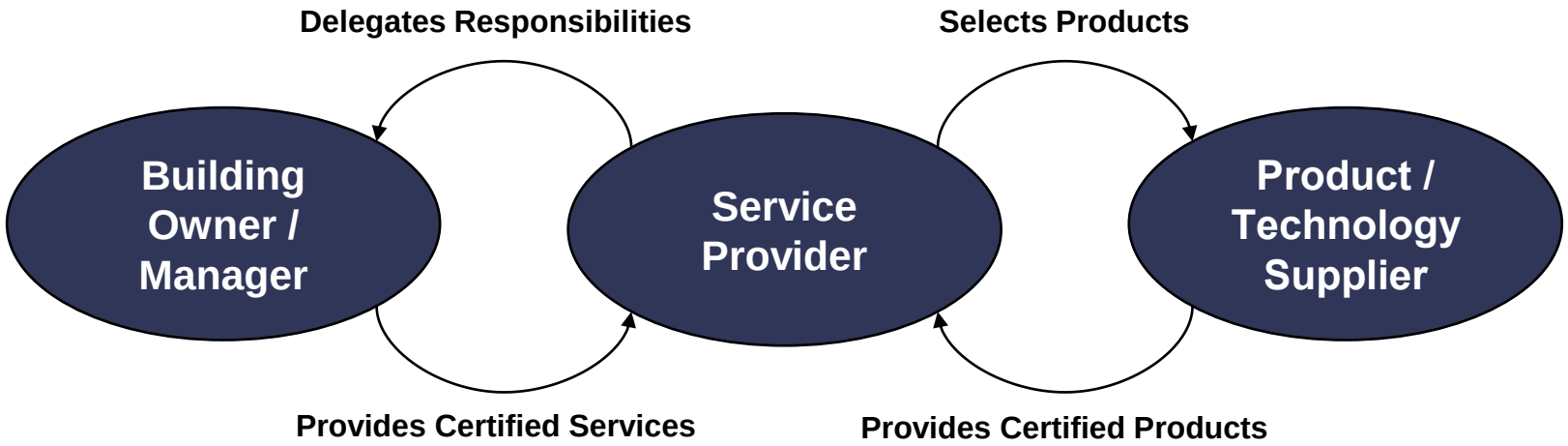
The BCS Framework is Based on Existing Standards and Controls



BCS Assessment Prerequisites

- Established OT/IT security governance initiative
- Asset inventory
- Service provider inventory
- Risk assessment that includes OT/IT
- Partitioned assets into Zones and Conduits (segmentation)

Roles and Responsibilities



Examples

- building owner
- building property managers

Standards

- ISA/IEC 62443-2-1 Owner
- ISA/IEC 62443-2-2 SPS
- ISA/IEC 62443-3-3 Systems

Certification/conformance

- BCS

Examples

- system integrators
- maintenance providers

Standards

- ISA/IEC 62443-2-4 Services
- ISA/IEC 62443-3-3 Systems

Certification/conformance

- IECEE

Examples

- building automation suppliers
- control system suppliers
- building physical systems suppliers

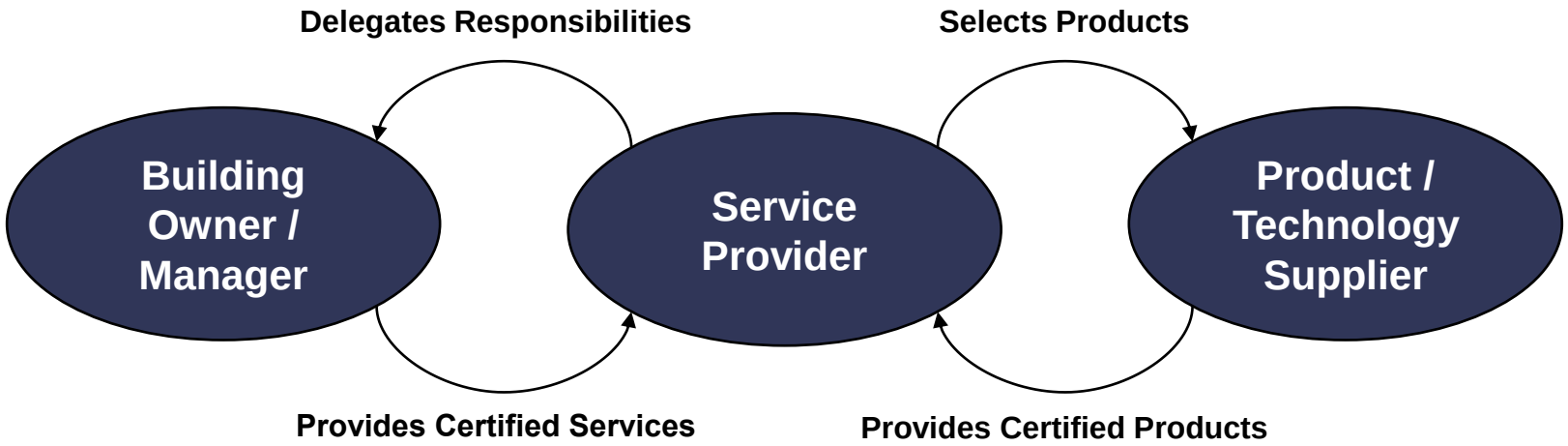
Standards

- ISA/IEC 62443-4-1 SDL
- ISA/IEC 62443-3-3 Systems
- ISA/IEC 62443-4-2 Components

Certification/conformance

- ISASecure
- IECEE

Roles and Responsibilities



Examples

- building owner
- building property managers

Certification/conformance

- BCS

Examples

- system integrators
- maintenance providers

Certification/conformance

- IECEE

Examples

- building automation suppliers
- control system suppliers
- building physical systems suppliers

Certification/conformance

- ISASecure
- IECEE

OT Assessment Scheme

ISA International Society of Automation

ISA/IEC 62443

ISASecure®

BUILDING Cyber Security

- BRONZE
- SILVER
- GOLD
- PLATINUM

Why Use ISA/IEC 62443 for OT Security?

The consequences of a security breach are different for IT and OT

- IT consequences include information security risk
- OT consequences include information and *physical risk*, e.g.:
  - loss of life/health
  - damage to equipment under control
  - damage to the environment
  - loss of product integrity

ISA/IEC 62443 is risk based

- Security Level is based on risk assessment process
- Segmentation into Zones and Conduits

ISA/IEC 62443 is widely adopted

- International standard
- Used in multiple industries (e.g. processing, manufacturing, transportation, medical)
- Products certified to comply with 62443 are available (e.g. ISASecure)

OT Design Principles: CRE Profile

Develop an OT cybersecurity conformance scheme for Commercial Real Estate

- facilitate the understanding of security principles by building owners (and stakeholders)
- assist BCS assessors in understanding the BCS rating system
- first vertical segment is commercial real estate

Based on ISA/IEC 62443 Series, which is specifically aligned with OT

- Part 2-1 for Building Owner requirements (draft)
- Part 2-2 for Security protection ratings (draft)
- Part 3-2 for Cybersecurity risk assessment process
- Part 2-4 for Integration and Maintenance Service Providers
- Part 3-3 for System technical security requirements

Reference Models

- Independent Building Control Zones
- Integrated Building Automation System (IBAS)
- Internet of Things (IoT) Building Automation System (IoTBAS)
- As-built Zone and Conduit model can use elements from each

Risk Assessment – Consequences and Impact

Health/Safety/Environmental		Reputation/Brand		Financial		Productivity		Regulatory	
What is the disruption of business operations and outage impact?	Score	How is reputation/brand affected and what is the reduction in cutomers and revenue due to loss of confidence?	Score	What are the projected financial losses? Possible gain for adversary vs. loss to owner/operator.	Score	What is the disruption of business operations and outage impact?	Score	What is the cost of corrective action, fines, and legal judgement?	Score
Serious long term health implications/Occupant loss of life.	4	Reputation is irrevocably or Severely destroyed or damaged. Irrecoverable or Severe reduction in existing and potential customers	4	Irrecoverable or severe Financial Loss.	4	Disruption of Business Operations Resulting in Unprocessed sales and Cleints.	4	Irrecoverable or Severe Corrective Action. Irrecoverable or Severe Fines or Legal Judgment.	4
Prevention of creating health risk focal point/Occupant injury.	3	Reputation is severly damaged, and significant effort and expense is required to recover. Significant reduction in clients and candidates.	3	Significant Financial Loss.	3	Disruption of Business Operations Resulting in Significant Delay in Candidate and Client Processing.	3	Significant Corrective Action cost. Significant Fine or Legal Judgment.	3
Occupant health impacted.	2	Reputation is damaged, and some effort and expense is required to recover. Some reduction in clients and candidates.	2	Some Financial Loss.	2	Disruption of Business Operations Resulting in Some Delay in Candidate and Client Processing.	2	Some Corrective Action costs. Some Fine or Legal Judgment.	2
Occupant discomfort.	1	Reputation is minimally affected; little or no effort or expense is required to recover. Minimal reduction in clients and candidates.	1	Minimal Financial Loss.	1	Disruption of Business Operations Resulting in Minimal Delay in Candidate and Client Processing.	1	Minimal Corrective action Costs. Minimal Fine or Legal Judgment.	1

Essential Functions

Property Damage example

Risk Assessment - Likelihood

- Risk = function of { Likelihood, Impact }
- Cybersecurity Likelihood = function of { P(Threat), P(Accessibility), P(Vulnerability) }
- Likelihood Assumptions
  - Threats are everywhere and have the means and motive to attack building control systems
    - Assume - P(Threat) = 1.0 (100%)
  - Building control systems have vulnerabilities, either known (unpatched), or unknown (zero-day)
    - Assume - P(Vulnerability) = 1.0 (100%)
  - Base overall likelihood on Accessibility to the Zone (Attack Surface)
- Cybersecurity risk = function of { P(Accessibility), Impact }

Accessibility Level	Description	Example
1	Low	Physical access only
2	Moderate	OT access (e.g. IBAS)
3	High	IT access
4	Very High	Public access (e.g. Internet)

Risk Assessment – Target Security Level

Target Security Level		Accessibility Level			
		1 - Low	2 - Moderate	3 - High	4 – Very High
Impact Level	4	SL 2	SL 3	SL 4	SL 4
	3	SL 2	SL 3	SL 3	SL 4
	2	SL 1	SL 2	SL 2	SL 3
	1	SL 1	SL 1	SL 2	SL 2

BCS Assessment Overview

Preparation

- Establish security program
- Inventory service providers
- Inventory assets including criticality
- Partition assets into zones and conduits
- Identify essential functions zones
- Perform risk assessment for each zone
  - Assess consequences
  - Assess likelihood (accessibility)
  - Determine Target Security Level

Assessment

- For each IT Zone
  - Assess IT security controls based on CIS Controls v8
- For each OT Zone
  - Assess owner security measure and maturity
  - Assess service provider security measures and maturity
  - Assess technical security measures based on Target Security Level

		Bronze	Silver	Gold	Platinum
OT Zones	Essential Function Zones	62/90	62/90	62/90	62/90
	Standard Zones	56/85	56/85	56/85	56/85
	Minimum Maturity Level	Repeatable	Repeatable	Repeatable	Improving
IT Zones	CIS Implementation Group	IG1 58/156	IG2 133/156	IG3 156/156	IG3 156/156

Building Functional Areas (Zones)

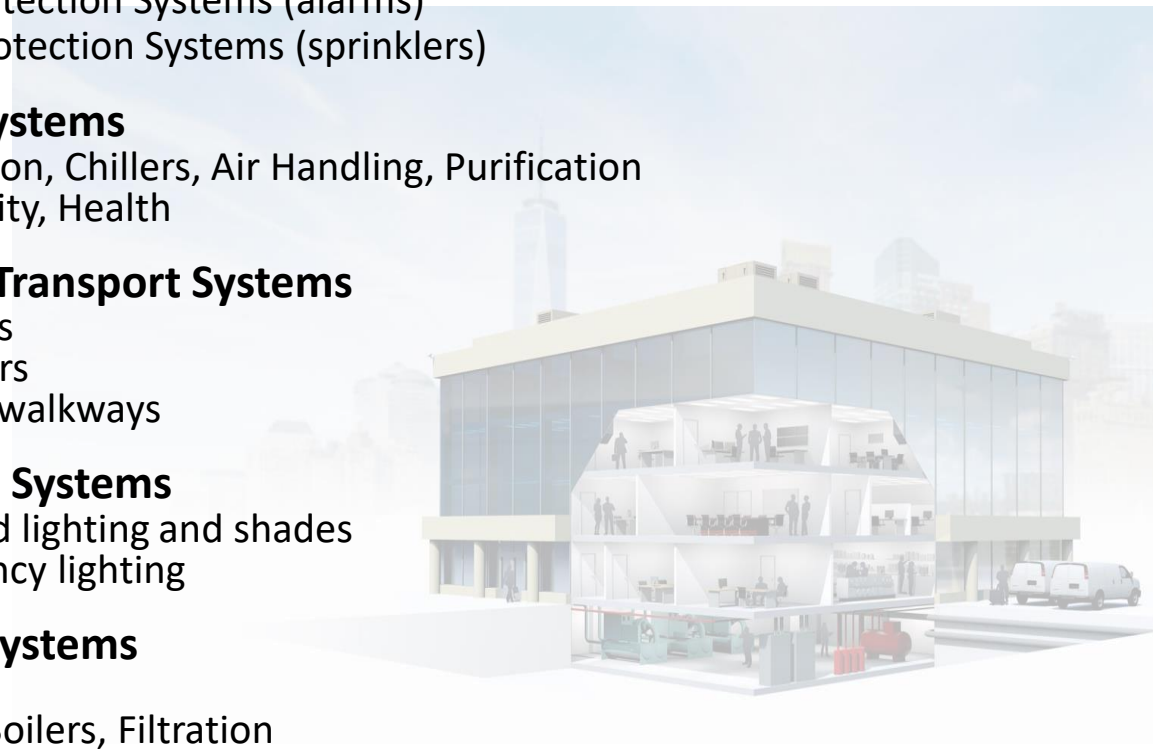
Fire Systems
- Fire Detection Systems (alarms)
- Fire Protection Systems (sprinklers)

HVAC Systems
- Ventilation, Chillers, Air Handling, Purification
- Air Quality, Health

People Transport Systems
- Elevators
- Escalators
- Moving walkways

Lighting Systems
- Standard lighting and shades
- Emergency lighting

Utility Systems
- Gas
- Water, Boilers, Filtration
- Electric (including Backup Generators, UPS, Solar, Wind)



Physical Access Systems
- Physical Security Control
- Video Surveillance
- People Count

A/V and Digital Signage
- Room Management, Music, Directories

Voice Communication Systems
- Standard
- Emergency

Voice Communications (wired & wireless)

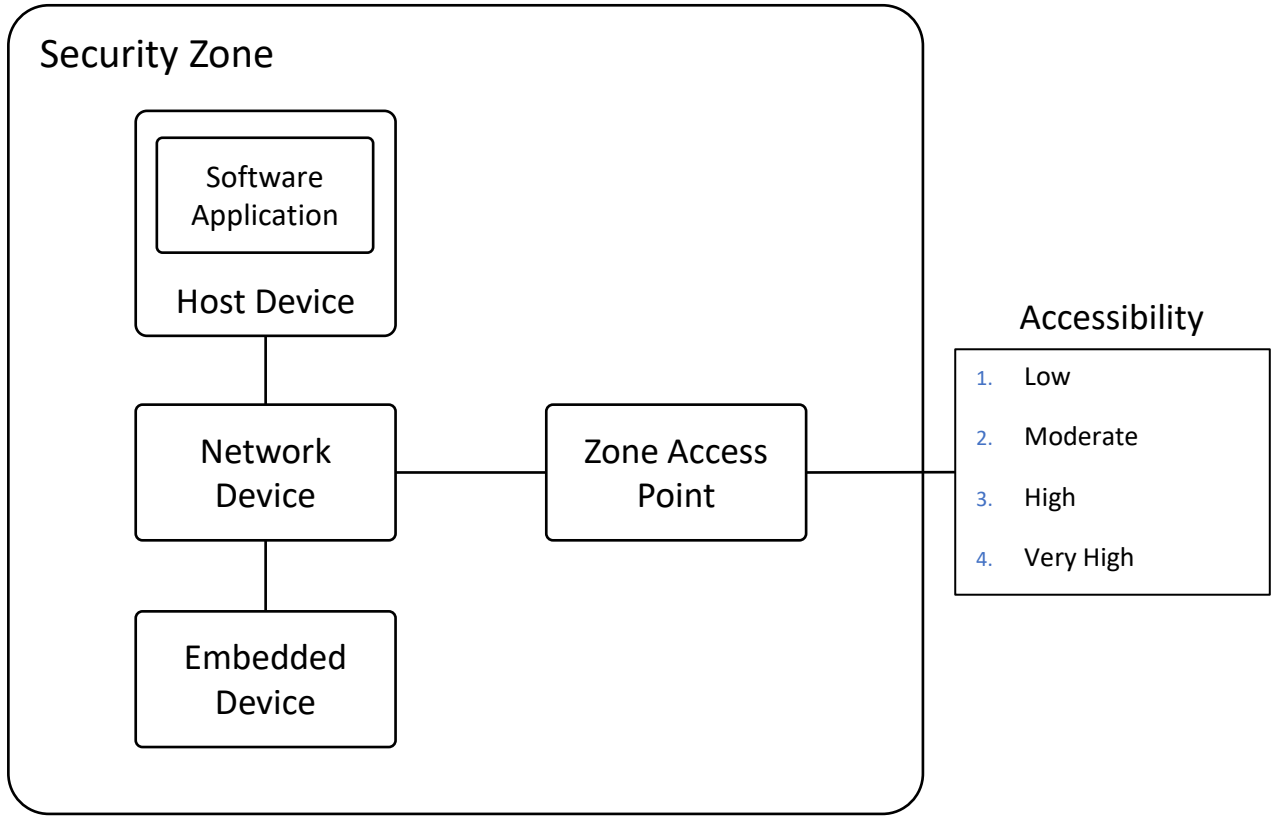
Parking Systems
- Access
- EV Charging

Building Automation Systems

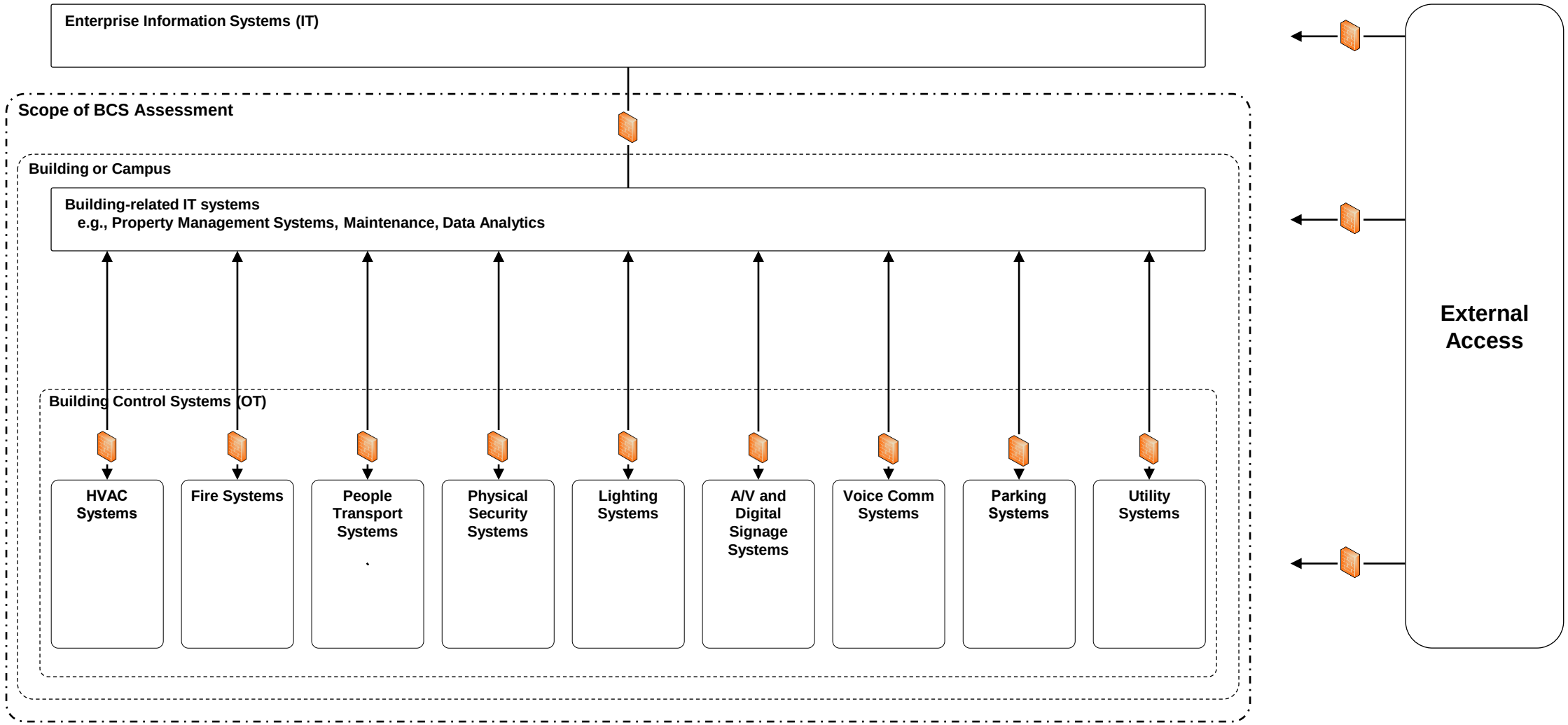
IT Systems
- Owner Network
- Property Management

Key Concept: Reference Model Security Zone

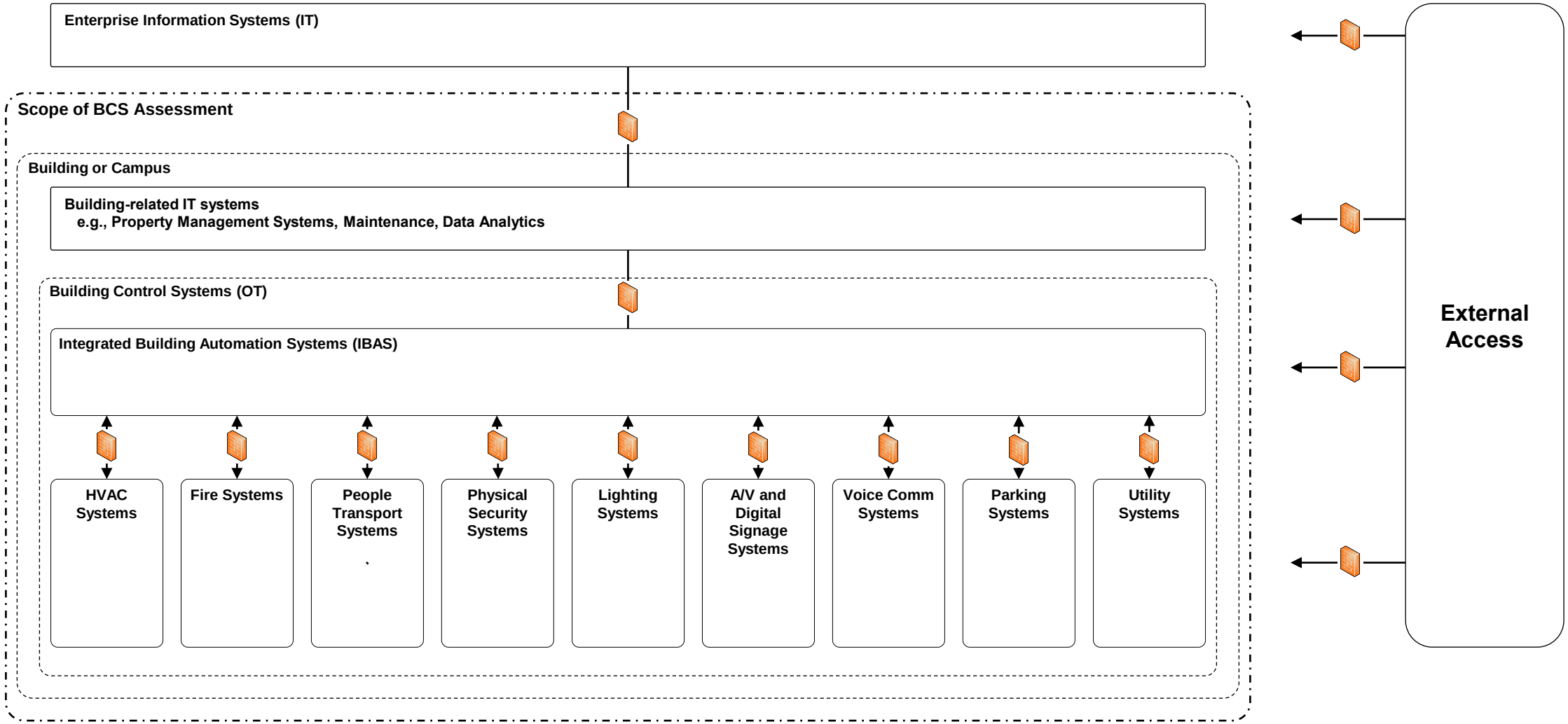
- Security Zone
  - set of assets with common security requirements
  - similar to network segmentation
- Components
  - Host device (e.g. Windows/Linux PC)
  - Software application (e.g. HMI)
  - Network device (e.g. switch, router)
  - Embedded device (e.g. PLC)
  - Zone access point (e.g. firewall)
- Accessibility types (in order of increasing risk)
  - Low (e.g. physical access, no network connection)
  - Moderate (e.g. physical access, network to/from OT zones)
  - High (e.g. physical access, network to/from IT zones)
  - Very High (e.g. physical access, network to/from Internet)
- Security Levels
  - allows selection of technical requirements based on risk
- Maturity Levels
  - maturity of policy, process, procedural requirements
- Essential Functions
  - Identify zones which have essential functions



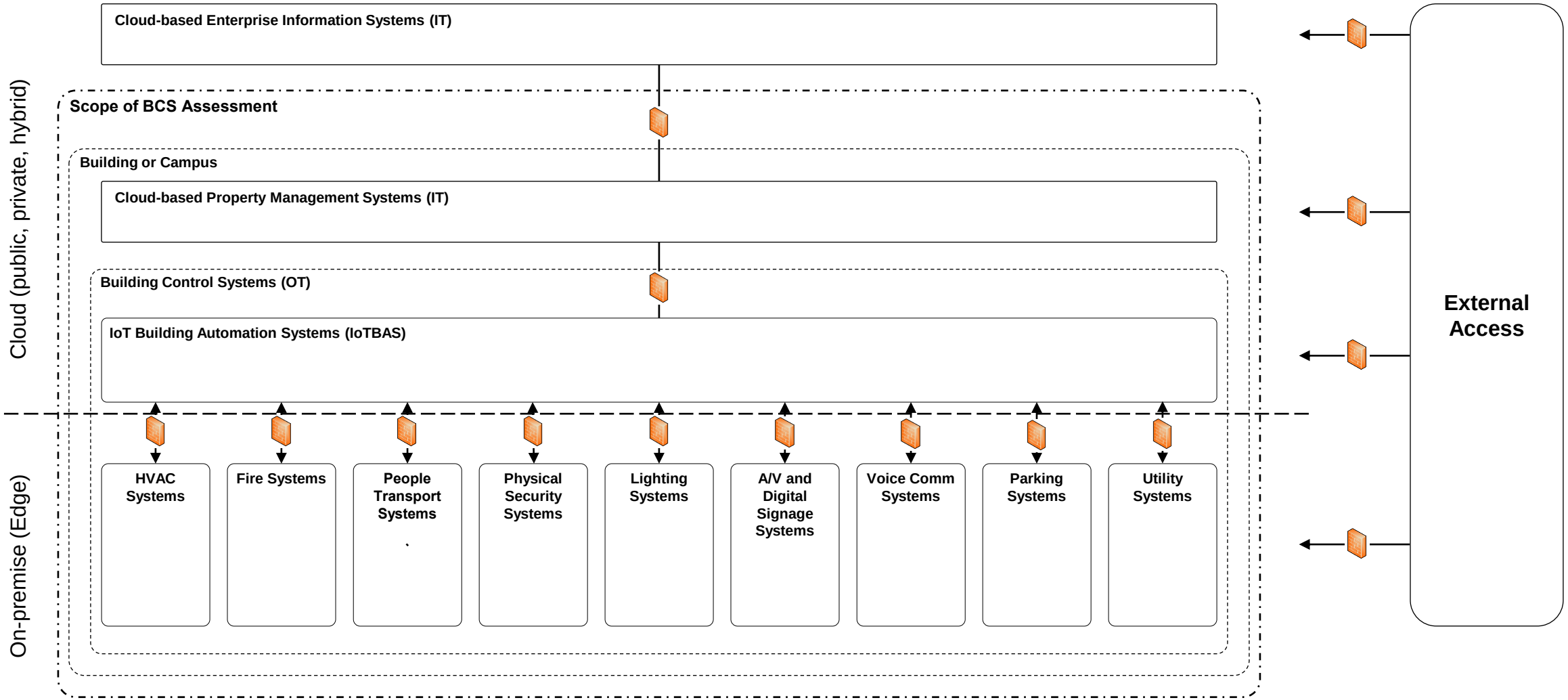
Reference Zone Model Independent Building Control System



Reference Zone Model Integrated Building Automation System (IBAS)



Reference Zone Model IIoT Building Automation System (IoTBAS)



IT Assessment Scheme

CIS Center for Internet Security®

NIST National Institute of Standards and Technology
Cybersecurity Framework

ISO 270001

BUILDING Cyber Security

- BRONZE
- SILVER
- GOLD
- PLATINUM

The Evolution of

2000 NSA/DoD Project

The Consensus Audit Guidelines (CSIS)

"The SANS Top 20" (the SANS Institute)

The Critical Security Controls (CCS/CIS)

2021 **The CIS Controls™**

CIS Implementation Groups

Crawl....(Bronze).....

IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

58
Cyber Defense Safeguards

Walk...(Silver).....

IG2 assists enterprises managing IT infrastructure with multiple departments and varied risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

75
Additional Cyber Defense Safeguards

Run...(Gold)...

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or minimize the impact of sophisticated attacks.

23
Additional Cyber Defense Safeguards

Total Safeguards **156**

IT Assessment Scheme: CIS Controls v8

Security Measures (controls) by Function

	Bronze	Silver	Gold	Platinum
Users	20	33	34	34
	10	29	36	36
	10	25	30	30
Data	8	16	21	21
	8	26	30	30
	2	4	5	5
Building Systems (OT)	64	85	90	90
Grand Total	122	218	246	246

BCS Assessment …Getting Started

- Establish OT/IT security governance initiative
- Asset inventory
- Service provider inventory
- Risk assessment that includes OT/IT
- Partitioned assets into Zones and Conduits (segmentation)

A Special Thanks to the “Breakfast Club”

- ❖ 600+ volunteered man hours
- ❖ 15+ Technical reviews (Pink Teams)
  - CRE Owners – MetLife, CA Ventures, COPT
  - System Integrators – McKenny’s
  - Tech Suppliers – Otis, Eaton, Schneider Electric, JCI (Simplex Grinnell) , Amazon
  - NIST/MITRE
  - TIA/UL
  - CRE Consultants

BEYONDEDGE

KMC CONTROLS

NOZOMI NETWORKS

PARTNER Engineering and Science, Inc.

Veridify Security

THE MINER AGENCY

Johnson Controls

INTELLIGENT BUILDINGS

NEMA National Electrical Manufacturers Association

ISASecure

Digitalware

CIS Center for Internet Security

BUILDING Cyber Security

Team

- ❖ Jason Christman
- ❖ Fred Gordy
- ❖ Steve Griffith
- ❖ Johan Nye
- ❖ Sebron Partridge
- ❖ Robert Portvliet
- ❖ Tony Sager
- ❖ E.J. von Schaumburg

Closing Remarks

Thank You

Questions?