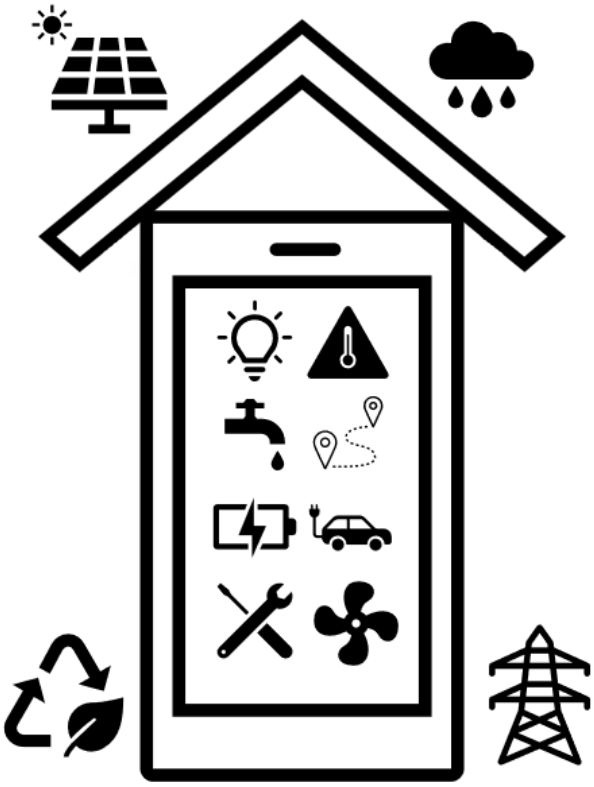


Interoperabiliteit, compatibiliteit en openheid binnen een Smart Building

Definities, aandachtspunten en aanbevelingen

Augustus 2021

SMART BUILDINGS IN USE

wtcb.be
Onderzoekt • Ontwikkelt • Informeert

AGENTSCHAP INNOVEREN & ONDERNEMEN

Vlaanderen
is ondernemen

Dit document werd opgesteld in het kader van de VLAIO IBN Cluster Smart Buildings In Use (Over de cluster - Smart Buildings In Use). Het kwam tot stand via de werkgroep 'Interoperabiliteit' binnen deze cluster. De visie die in dit document gegeven wordt, is de gedeelde visie van de cluster-leden. De werkgroep 'Interoperabiliteit' die bijdroeg aan dit document bestaat uit volgende leden:

Benedikt	Declercq	Vlaamse Confederatie Bouw
Ruben	Delvaeye	WTCB
Luc	François	WTCB
David	Grillet	WTCB
Michel	Grosemans	GIA
Alain	Mathijs	Trigrr
Peter	Van Schel	Procos Group
Benny	Vanvolsem	Honeywell Partner Channel
Stef	Vande Meulebroucke	Sumi Smart
Kris	Vanderbruggen	Schneider Electric (voordien: EEG)

Inhoud

1 Inleiding

De functionaliteit van een Smart Building is sterk afhankelijk van de mogelijkheid tot **interactie tussen** de verschillende **systemen** binnen het gebouw en de interactie met externe systemen (bv. energienetten, etc.). Ook de interactie tussen de componenten van een individueel systeem speelt een belangrijke rol in het bereiken van de gewenste functionaliteit.

Interoperabiliteit, compatibiliteit en openheid zijn begrippen die vaak opduiken wanneer over deze verschillende types interacties gesproken wordt. Hoewel de termen al eens in één adem genoemd worden, zijn het toch geen synoniemen van elkaar. Bovendien bestaat er niet 'één algemeen aanvaarde definitie' voor deze begrippen. De definitie van de begrippen is afhankelijk van de context en verschillende partijen gebruiken hun eigen definitie. Dit document tracht klaarheid te scheppen door de lezer **inzicht** te geven in de thematiek en in welke **problematieken** hieromtrent bestaan. Tot slot wordt er gekeken naar mogelijke **oplossingen**.

Er wordt, vertrekkende van een **technologische benadering** van Smart Buildings, gefocust op de systemen en componenten die aan de basis liggen van een Smart Building. Hierbij wordt uitgegaan van volgende omschrijvingen:

- **Interoperabiliteit:** de mogelijkheid tot interactie tussen systemen door middel van interpreteerbare informatie-uitwisseling
- **Compatibiliteit:** de mogelijkheid tot interactie tussen componenten binnen een systeem
- **Openheid:** de mate waarin informatie over de werking, functionaliteit en configuratie van een technologie beschikbaar, toegankelijk en bruikbaar is

Belangrijk binnen deze omschrijvingen is het **onderscheid tussen systemen en componenten**. Systemen zijn in staat om op zichzelf een bepaalde functie binnen een gebouw vervullen. Voorbeelden van systemen zijn o.a. een verlichtingssysteem, een verwarmingssysteem, een zaalreservatiesysteem, etc. Componenten kunnen als de bouwstenen van systemen gezien worden en hebben als afzonderlijke entiteit geen of een beperkte functie. Voorbeelden van componenten zijn onder ander een thermostaat, een bewegingssensor, een bedieningspaneel, …

In dit onderdeel wordt dieper ingegaan op de hierboven genoemde concepten. Er wordt gefocust op technische gebouwsystemen (bv. verwarming, verlichting, etc.), (hardware)componenten en digitale communicatie. Binnen een Smart Building is er eveneens nood aan softwaresystemen voor dataopslag en -verwerking en gebruikersinterfaces. Denk bijvoorbeeld aan databases, besturingssystemen, computerprogramma's, webapplicaties, mobiele apps en API's[1]. Hier gaat binnen dit document minder aandacht naartoe.

[1] Application Programming Interface: een manier om softwaresystemen te laten communiceren

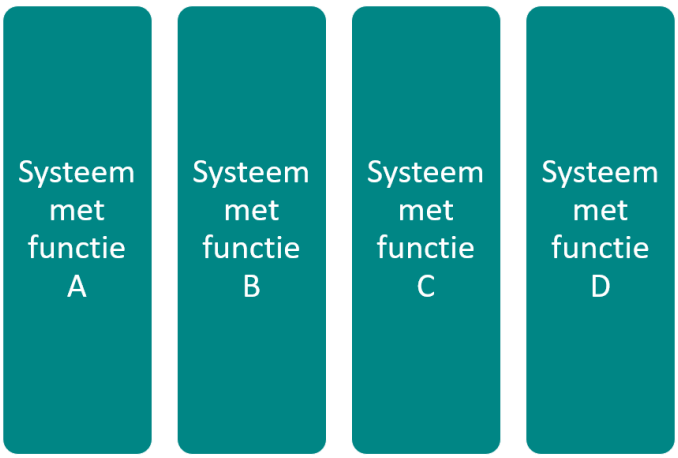
Bij het beschrijven van de concepten zal gesproken worden over standaarden en protocollen. Deze termen worden in hun nauwe, technische betekenis gebruikt. Er wordt uitgegaan van volgende omschrijvingen:

- **standaard:** een formeel, neergeschreven en gevalideerd technisch afsprakenstelsel dat gepubliceerd is door een algemeen erkende organisatie
- **(telecommunicatie)protocol:** een verzameling van technische regels en afspraken die toelaten om informatie uit te wisselen over een communicatiemedium[2]

[2] Voorbeelden van communicatiemedia voor bedrade communicatie zijn bv. kabels met getwiste koperparen, optische vezelkabels, coaxiale kabels, etc. Bij draadloze communicatie worden meestal radiogolven gebruikt als draadloos medium. Meer informatie hierover is terug te vinden in de appendix digitale connectiviteit van de Praktijkgids Smart Buildings

2 Silovorming

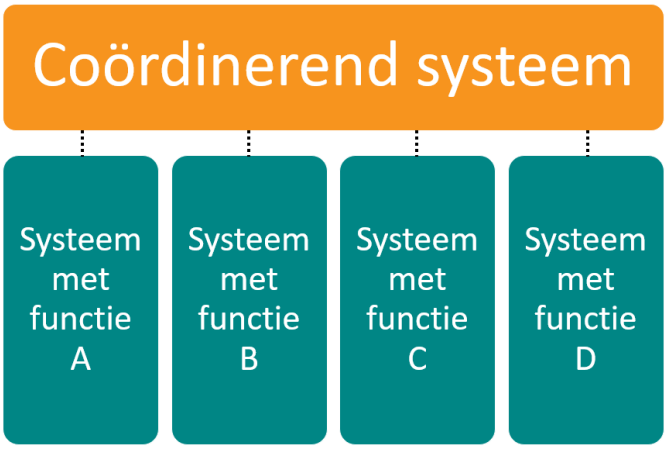
Een hedendaags gebouw bevat een **veelheid aan systemen**. Denk bijvoorbeeld aan de klassieke technische gebouwsystemen die instaan voor HVAC, verlichting, zonwering, toegangscontrole, etc., maar even goed softwaresystemen die o.a. instaan voor de interactie met de gebouwgebruiker. Wanneer deze systemen **naast elkaar** geïmplementeerd worden en er geen onderlinge samenwerking mogelijk is, wordt van **silovorming** gesproken (zie Figuur 1). De silo's komen overeen met de individuele systemen. Wanneer deze volledig losstaan van elkaar, worden er vaak aanzienlijke opportuniteiten gemist om meerwaarde te creëren onder andere op vlak van energie-efficiëntie, comfort, gebruikerservaring, onderhoud,… In een dergelijke implementatie kan men, afhankelijk van de geboden functionaliteit van de afzonderlijke systemen, spreken over slimme gebouwsystemen, maar niet over een slim gebouw.



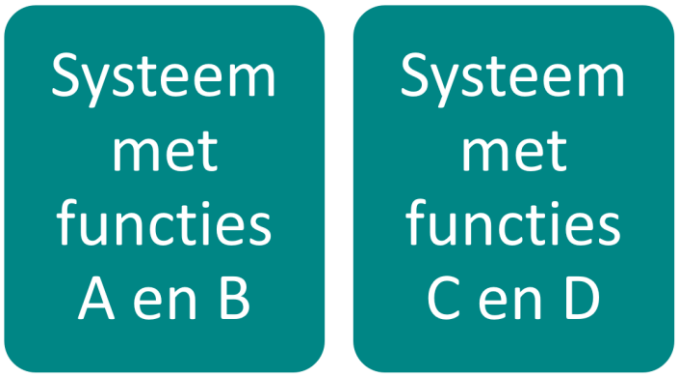
Figuur 1: Silovorming

In een Smart Building is de mogelijkheid tot interactie tussen de systemen die voor de diverse functies van het gebouw instaan cruciaal. Deze kan bijvoorbeeld bereikt worden via een **bovenliggend coördinerend systeem** dat de silo's met elkaar verbindt (zie Figuur 2). Een andere mogelijkheid bestaat erin om één of meerdere **grotere systemen** te voorzien, die de functies van meerdere afzonderlijke systemen vervullen en op die manier de silo's doorbreken (zie Figuur 3). Zowel de piste van het bovenliggende systeem als deze van grotere systemen vereisen dat er interactie mogelijk is tussen componenten en/of systemen.

De manier waarop binnen een Smart Building de silo's zich tot elkaar verhouden is vaak bepaald door technologische limieten maar ook aspecten als veiligheid, wetgeving, kost, etc. kunnen meespelen. Verregaande integratie laat toe om de mogelijkheden van Smart Buildings ten volle te benutten, maar brengt ook uitdagingen met zich mee zoals complexiteit van de implementatie en het beheer en onderhoud van coördinerende systemen, databeheer, dataveiligheid, privacy… Zo zullen systemen voor brandveiligheid, inbraakdetectie en liftsystemen vaak bewust aparte silo's vormen die slechts beperkte interactie met andere systemen toelaten.



Figuur 2: Interactie tussen de silo's via een bovenliggend systeem



Figuur 3: Doorbreken van de silo's via grotere systemen

Op technologisch vlak, zou een mogelijke oplossing om ervoor te zorgen dat componenten en/of systemen kunnen interageren, een universele standaard zijn waaraan alle systemen en componenten voldoen. In praktijk bestaan er vandaag **meerdere al dan niet gestandaardiseerde protocollen** die interactie tussen systemen en componenten mogelijk maken. Zo kan gebruik gemaakt worden van digitale elektrische signalen bv. via een schakelaar of relais contact, analoge elektrische signalen via spanning of stroomvariaties bv. 0-10 V of 4-20 mA maar ook meer geavanceerde protocollen zoals BACnet, KNX, Lonworks, Modbus, DALI, EnOcean, Bluetooth, Zigbee, Thread, fabrikant-specifieke protocollen, etc.). Bepaalde protocollen zoals BACnet MS/TP of Zigbee zijn bedoeld voor interactie tussen componenten terwijl protocollen zoals BACnet/IP eerder ingezet worden voor interactie tussen systemen. Elk van deze protocollen zijn bovendien ontwikkeld met bepaalde use cases in gedachten. Sommige protocollen zijn specifiek voor één domein ontwikkeld (bv. DALI: kunstverlichting, M-bus: verbruiksmeters, …) terwijl andere zoals BACnet en KNX gebruikt kunnen worden binnen meerdere domeinen (bv. HVAC, zonwering, energiemonitoring, etc.).

Er bestaat **geen kant-en-klare aanpak** voor het fenomeen van silovorming. Binnen een Smart Building is het gebruik van technologische oplossingen gebaseerd op verschillende protocollen en standaarden dan ook te verwachten. Om de oplossingen goed te kunnen evalueren, is het belangrijk om rekening te houden met aspecten als coëxistentie, interoperabiliteit, compatibiliteit en openheid. Ook de organisatorische aspecten die gepaard gaan met de keuze, de implementatie en het gebruik van technologische oplossingen verdienen de nodige aandacht.

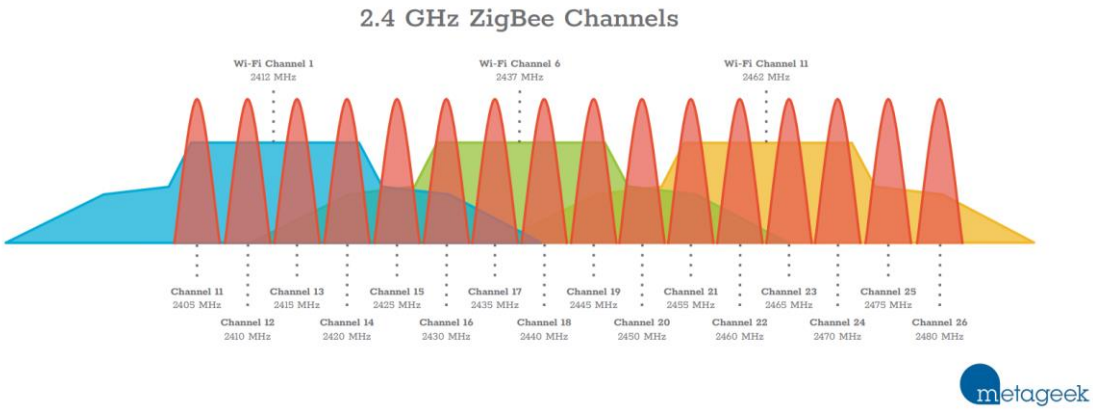
3 Coëxistentie

Coëxistentie wordt vanuit de cluster 'Smart Buildings in Use' gedefinieerd als het **naast elkaar bestaan** van verschillende systemen zonder dat deze elkaars werking negatief beïnvloeden. Het kan gezien worden als **een eerste stap** naar interoperabiliteit. Immers, wanneer systemen elkaars werking negatief zouden beïnvloeden, is succesvolle samenwerking tussen de systemen slechts beperkt of helemaal niet mogelijk.

Coëxistentie op de fysieke laag (zoals in het OSI model[3]) houdt in dat de elektromagnetische signalen van systemen die een eigen medium gebruiken, elkaar niet beïnvloeden. Concreet kan dit voor **bedrade systemen** betekenen dat **afzonderlijke kabels** gebruikt worden (bv. buskabels) of dat verschillende spectrumbanden gebruikt worden binnen een kabel (bv. binnen coaxiale kabel of glasvezelkabel). In bepaalde gevallen worden afgeschermde kabels gebruikt om het risico op elektromagnetische **interferentie** te **vermijden** (bv. afschermde kabel met getwiste aderparen).

Ook voor **draadloze systemen** kan coëxistentie binnen de fysieke laag bereikt worden, en dit op verschillende manieren. Zo kan bijvoorbeeld gebruik gemaakt worden van **gescheiden spectrumbanden** (bv. Wi-Fi netwerken die gebruik maken van de 2.4 GHz en de 5Ghz band). Ook binnen eenzelfde band kan coëxistentie bereikt worden, bijvoorbeeld via slimme kanaalkeuze (bv. Zigbee en Wi-Fi netwerken binnen de 2.4 GHz band, zie Figuur 4) of via het toepassen van technologie om **interferentie** te **beperken** (bv. Bluetooth en Wi-Fi binnen de 2.4 GHz band).

Noteer dat coëxistentie ook mogelijk is tussen systemen voor data-overdracht en systemen voor stroomvoorziening. Denk bijvoorbeeld aan USB kabels, netwerkkabels die gebruik maken van 'Power over Ethernet' (PoE) of het draadloos laden van een smartphone.



Figuur 4: Coëxistentie Wi-Fi (blauw, groen en geel) en Zigbee (rood) in de 2.4 GHz band. Bron: (ZigBee and WiFi Coexistence)

Wanneer systemen geen nood hebben aan een individueel fysiek medium, kunnen deze gebruik maken van dezelfde infrastructuur. Zo zouden traditionele IT systemen in theorie bijvoorbeeld hetzelfde netwerk kunnen gebruiken als IP-gebaseerde gebouwsystemen of zouden binnen een IP-netwerk voor gebouwsystemen systemen die gebruik maken van verschillende communicatieprotocollen naast elkaar kunnen bestaan (bv. KNXnet/IP en BACnet/IP). In de praktijk

[3] Het OSI model is een raamwerk dat gebruikt wordt om de verschillende functies binnen een digitaal communicatiesysteem onder te verdelen. Een ander vaak gebruikt model is het TCP/IP model. Meer informatie over deze modellen is terug te vinden in de appendix digitale connectiviteit van de Praktijkgids Smart Buildings

wordt echter meestal een gescheiden fysiek medium voorzien voor gebouwsystemen gezien een fysieke scheiding het netwerkbeheer voor de klassieke IT diensten vergemakkelijkt. Ook worden de risico's m.b.t. cyberveiligheid vaak geacht beperkter te zijn.

Het aantal en de aard van de systemen die gebruikt worden binnen een Smart Building zullen een invloed hebben op de haalbaarheid van coëxistentie. Naast de bovengenoemde aspecten wordt er best ook rekening gehouden met eventuele **toekomstige noden** qua capaciteit en omvang van systemen. Zo kan een uitbreiding of een verhoging van de capaciteit van een systeem een impact hebben op de coëxistentie met andere systemen. Infrastructuur heeft immers altijd limieten. Denk bijvoorbeeld aan een uitbreiding van een camerabewakingssysteem binnen een gedeeld IP netwerk (dat een eindige capaciteit heeft). Meestal zullen nefaste combinaties van systemen resulteren in een lagere haalbaarheid van coëxistentie, maar in bepaalde gevallen kunnen deze ook resulteren in een totaal gebrek aan coëxistentie.

Naast de communicatie-infrastructuur zijn er ook andere domeinen die bepalend kunnen zijn voor coëxistentie. Zo kunnen gebouwsystemen ook met elkaar interfereren op gebied van de functionele objectieven. Bijvoorbeeld: een verlichtingssysteem kan een bepaalde hoeveelheid warmte afgeven. Deze kan mogelijks een invloed hebben op de hoeveelheid warmte of koude die een HVAC systeem moet leveren.

4 Compatibiliteit en uitwisselbaarheid

Compatibiliteit duidt op verenigbaarheid en wordt vanuit de cluster 'Smart Buildings in Use' gedefinieerd als de mogelijkheid tot samenwerking tussen componenten **binnen een systeem**.

Uitwisselbaarheid is de mogelijkheid om een (software)onderdeel of (hardware)component te vervangen door een ander (meestal nieuwer) exemplaar.

Er bestaan verschillende **niveaus van uitwisselbaarheid**. Bij absolute uitwisselbaarheid is het mogelijk de vervanging door te voeren zonder enige impact op de werking van het systeem en zonder dat enige (her)programmatie nodig is. In praktijk zal het niveau van uitwisselbaarheid meestal lager liggen. Een vervanging zal vaak wel een zekere invloed hebben op de werking van het systeem en/of enige (her)programmatie vereisen.

Er zijn verschillende **soorten uitwisselbaarheid**. Zo is het mogelijk om een onderdeel binnen een systeem te vervangen door een identiek exemplaar of een exemplaar met identieke eigenschappen. In andere gevallen wordt er bij het vervangen gekozen voor een nieuwe versie van de component die over nieuwe eigenschappen en/of mogelijkheden beschikt. In dit laatste geval is achterwaartse (ook wel neerwaartse) compatibiliteit ('**backward/downward compatibility**') belangrijk. Deze term duidt op de eigenschap van een nieuwe component om compatibel te zijn met de bestaande (oudere) componenten in een systeem. Deze eigenschap zorgt er onder andere voor dat het ondanks een evolutie van een standaard, protocol of technologie, niet per se nodig is om alle bestaande componenten in een systeem te vervangen. Een voorbeeld hiervan is het Wi-Fi-protocol. Zo is Wi-Fi 6 achterwaarts compatibel met Wi-Fi 5, wat bijvoorbeeld betekent dat je bestaande componenten die gebruik maken van Wi-Fi-5 kan verbinden met een Wi-Fi 6 access point. Achterwaartse compatibiliteit zorgt er dus voor dat een nieuwe component bestaande functionaliteit van oudere componenten blijft ondersteunen. Dit sluit niet uit dat deze nieuwe component bijkomende functionaliteit kan bieden. De oudere componenten kunnen deze nieuwe functionaliteiten echter niet gebruiken.

Bij het vervangen van componenten waarop een configuratie opgeslagen is (bv. een DALI gateway) dient men speciale aandacht te besteden aan de **overdraagbaarheid** van deze **configuratie**. Een component kan voor de interactie met andere componenten weliswaar gebruik maken van een protocol dat de uitwisselbaarheid vergemakkelijkt, maar de implementatie van de configuratie in een component en het exporteren en inladen ervan is zo goed als altijd fabrikant-specifiek. Hierdoor is het vervangen van een geconfigureerde component door een exemplaar van een andere fabrikant zelden een 'plug and play' ervaring.

Ook van belang bij uitwisselbaarheid van componenten is de mogelijke aanwezigheid **van fabrikant-specifieke functionaliteiten of protocollen**. Sommige protocollen (bv. Modbus, DALI) voorzien de mogelijkheid voor een fabrikant om bepaalde functionaliteiten vrij in te vullen of toe te voegen. Daarnaast kunnen componenten soms tegelijkertijd gebruik maken van zowel gestandaardiseerde/open als gesloten protocollen. Indien een component van een fabrikant-specifieke feature binnen een gestandaardiseerd/open protocol of van een combinatie van gestandaardiseerde/open en gesloten protocollen gebruik maakt, zal een uitwisseling met een niet-backward-compatibele component van dezelfde fabrikant, of een component van een andere fabrikant, resulteren in een functionaliteitsverlies.

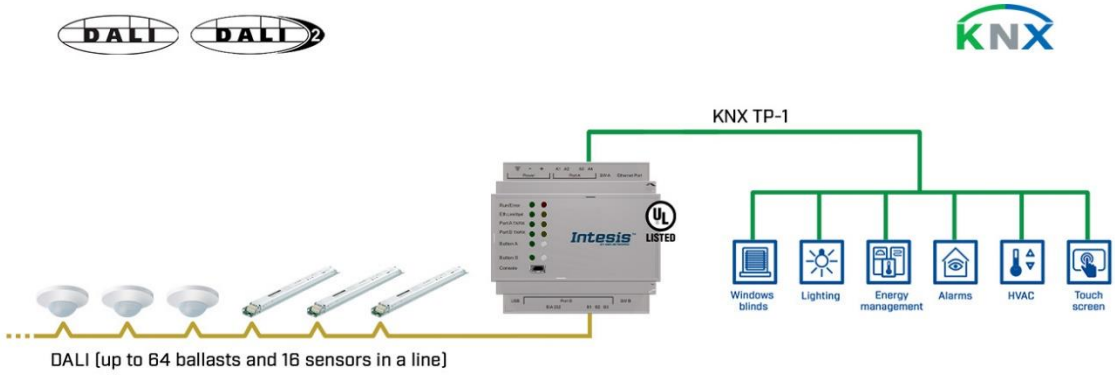
5 Interoperabiliteit

Interoperabiliteit wordt vanuit de cluster 'Smart Buildings in Use' gedefinieerd als de mogelijkheid tot interactie **tussen individuele systemen** door middel van informatie-uitwisseling.

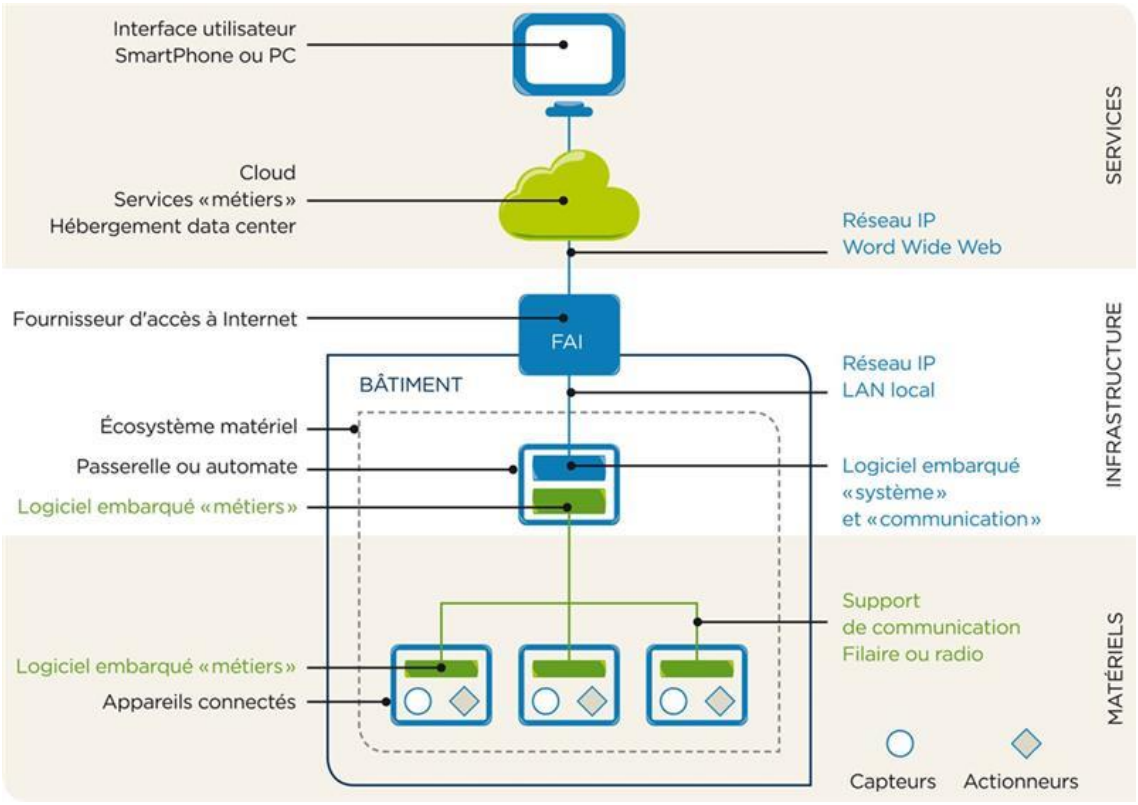
Belangrijk hierbij is dat de informatie ook correct geïnterpreteerd kan worden, m.a.w. de systemen moeten de mogelijkheid hebben iets te doen met de ontvangen informatie. Toegepast op Smart Buildings gaat interoperabiliteit over de interactie tussen de verschillende systemen (bv. verlichting, verwarming, externe systemen, coördinerende systemen, …). Het is deze interactie die meerwaardecreërende toepassingen zal mogelijk maken onder andere op vlak van energie-efficiëntie, comfort, gebruikerservaring, onderhoud, etc. Achter de schermen kan een hoge graad van interoperabiliteit ook toelaten om de functie van een component binnen een individueel systeem (bv. sensor voor aanwezigheidsdetectie) te delen met andere relevante systemen (bv. verlichting, verwarming, zaalreservatie, …) en op die manier, waar relevant, een vermenigvuldiging van componenten vermijden.

Om interoperabiliteit van digitale systemen te bekijken, wordt vaak gebruikt gemaakt van gelaagde communicatiemodellen zoals het OSI model of het TCP/IP model. Dergelijke modellen laten toe om verschillende vormen van interoperabiliteit beter te definiëren. Voor bepaalde technische systemen kan het voldoende zijn om interoperabiliteit te voorzien op slechts een aantal lagen. Zo is het voor afzonderlijke IP-netwerken voldoende om interoperabel te zijn tot en met de netwerklaag (OSI-lagen 1 t.e.m. 3). Voor toepassingsgerichte systemen is het echter noodzakelijk om **interoperabiliteit** te voorzien **tot op het niveau van de applicatielaag** (OSI laag 7). Het is deze laatste laag die zal verzekeren dat systemen niet enkel informatie kunnen uitwisselen, maar deze ook kunnen interpreteren.

Een eerste mogelijkheid om interoperabiliteit tot in de applicatielaag te bereiken bij het gebruik van meerdere (al dan niet gestandaardiseerde) protocollen, is het voorzien van zogenaamde **gateways**. Een gateway maakt de vertaling tussen verschillende protocollen en kan ondergebracht zijn in een fysiek toestel of geïmplementeerd zijn in software. Een fysieke gateway zal typisch de vertaling maken tussen protocollen die verschillende fysieke media gebruiken (bv. KNX/TP en DALI, KNX/TP en KNX/IP, etc.), zie Figuur 5 voor een voorbeeld. Een softwarematige gateway daarentegen kan enkel de vertaling maken tussen protocollen die onderliggend dezelfde communicatielaag gebruikten (bv. MQTT en KNX/IP maken beide gebruik van IP).



Figuur 5: DALI – KNX fysieke gateway. Bron: (Intesis, 2021)



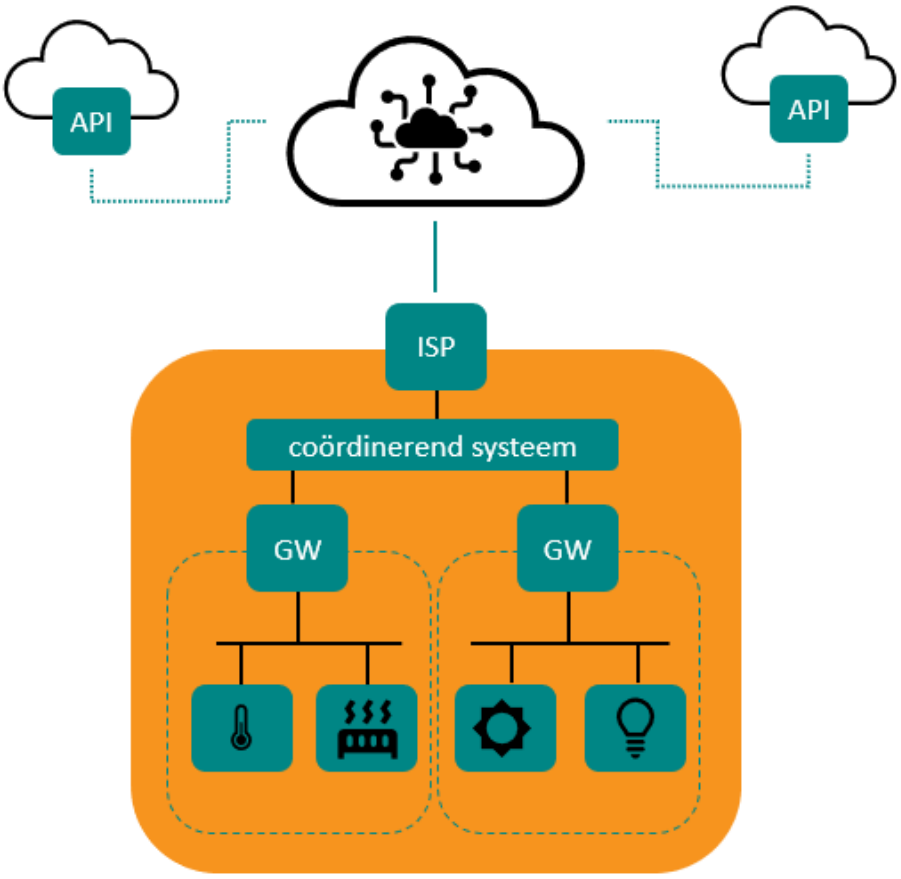
Figuur 6: Voorbeeld een Smart Building architectuur met gateways ('passerelle') en online diensten ('services'). Deze laatste interageren met het gebouw via API's. Bron: ((SBA), n.d.)

Een tweede mogelijkheid om interoperabiliteit tot in de applicatielaag te bereiken bij het gebruik van systemen die werken met verschillende (al dan niet gestandaardiseerde) protocollen bestaat erin om systemen die over IP connectiviteit beschikken, te voorzien van softwarematige koppelpunten ('interfaces') zoals bijvoorbeeld een **API** (Application Programming Interface). Via deze interface is interactie met andere gebouwsystemen of softwarecomponenten mogelijk waardoor er een grotere interoperabiliteit ontstaat. Deze oplossing is, samen met een IP netwerk voor gebouwsystemen, bijvoorbeeld de vereiste die binnen het van oorsprong Franse Ready2Services (R2S) raamwerk gesteld wordt om interoperabiliteit te verzekeren (zie Figuur 6). Er bestaan verschillende soorten API's en software-interfaces. Om integratie van systemen te faciliteren, kan gebruik gemaakt worden van (open) standaarden (bv. voor data-interfaces, datamodellen, data-opslag, …) en is een goede documentatie aangeraden.

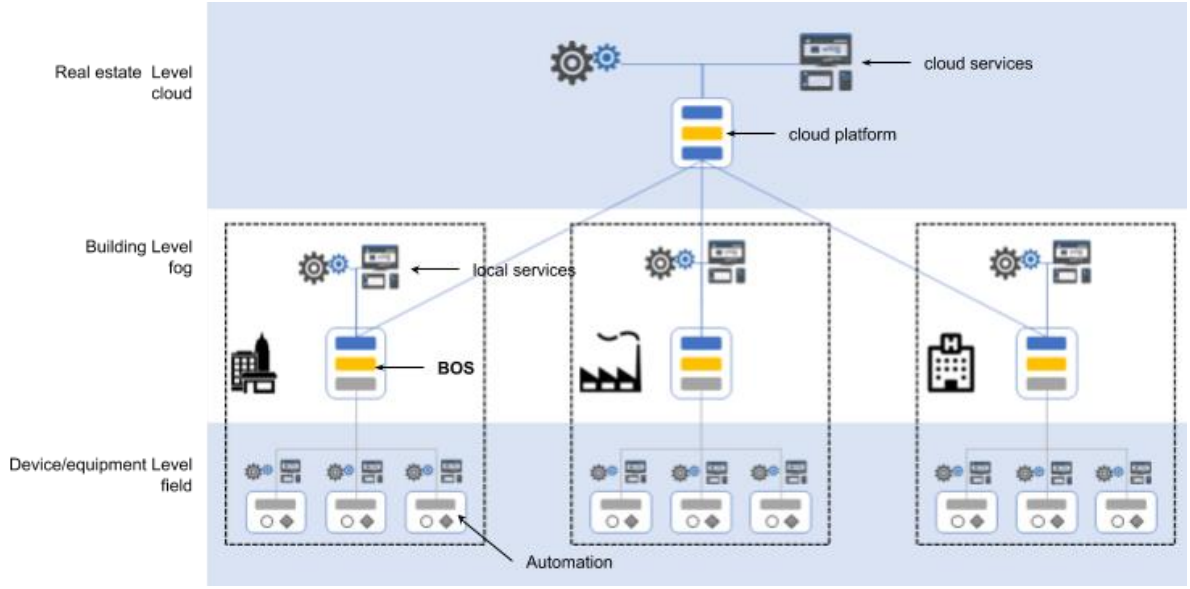
Gebruik makende van deze twee mogelijkheden kan interoperabiliteit over of doorheen de silo's bereikt worden. Zo is het bijvoorbeeld mogelijk om een bovenliggend coördinerend systeem te voorzien dat een koppeling maakt met de nodige onderliggende gebouwsystemen. Op die manier hoeft elk gebouwsysteem slechts één koppelpunt ('**interface**') te voorzien. Het coördinerende systeem kan een bijvoorbeeld een gebouwbeheersysteem (GBS) of op hoger niveau een zogenaamd Building Operating System (BOS) zijn[4]. Op die manier kan ook gemakkelijk de koppeling gemaakt worden naar bovenliggende softwaresystemen die bijkomende toepassingen toelaten (bv. gebruik makende van data-analyse en AI technieken). Deze softwaresystemen kunnen lokaal of in de cloud geïmplementeerd worden (zie Figuur 7 en Figuur 8). Voor kleinere gebouwen of gebouwen waarin er

[4] Zie Praktijkgids - Smart Buildings In Use voor meer informatie over GBS en BOS.

slechts beperkte Smart Building functionaliteit voorzien wordt, kan het voldoende zijn om systemen rechtstreeks met elkaar te koppelen via gateway- en/of API-oplossingen.



Figuur 7: Voorbeeld van een Smart Building architectuur met gateways (GW) en toegang tot clouddiensten via een Internet Service Provider (ISP) en Application Programming Interfaces (API)



Figuur 8: Voorbeeld van een Smart Building architectuur met een Building Operating System (BOS), lokale diensten en clouddiensten. Bron: (Bellec, 2019)

Bij het ontwerp van een interoperabele oplossing voor een slim gebouw is het belangrijk om goed na te denken over de **functionele vereisten** en hoe deze zich vertalen in **technische vereisten**: welke meerwaarde-creërende toepassingen moeten geïmplementeerd (kunnen) worden binnen het gebouw, welke systemen moeten hiervoor met elkaar kunnen interageren, welke data moet uitgewisseld worden, met welke frequentie, etc. ? Voldoende reflectie bij deze vragen zal toelaten om tot een **doeltreffende oplossing** te komen die **geen onnodige complexiteit** introduceert.

6 Openheid

Openheid wordt vanuit de cluster 'Smart Buildings in Use' gedefinieerd als de **mate waarin informatie** over de werking, functionaliteit en configuratie van een technologie **beschikbaar, toegankelijk en bruikbaar is**. Dit is bewust een brede definitie gezien openheid een breed concept is dat toepasbaar is op meerdere niveaus binnen een Smart Building. Zo wordt er gesproken over open protocollen, open interfaces, 'open source', etc.

Openheid is in de meeste gevallen een noodzakelijke voorwaarde om de nodige interoperabiliteit en/of compatibiliteit te kunnen bereiken. Bruikbare informatie over de werking van een systeem of component is immers noodzakelijk om er interactie mee mogelijk te maken. In dit onderdeel wordt dieper ingegaan op een aantal soorten openheid.

6.1 Openheid protocollen voor gebouwsystemen

6.1.1 Standaarden en open protocollen

Standaarden en open protocollen voor gebouwsystemen spelen een belangrijke rol bij het nastreven van compatibiliteit en interoperabiliteit. Deze worden typisch ontwikkeld via een **ontwikkelingsproces** waarbij **meerdere organisaties** betrokken zijn. De ontwikkeling en publicatie van een standaard gebeurt meestal onder **toezicht van een erkende organisatie**. Enerzijds zijn er standaarden die ontwikkeld en onderhouden worden door internationale organisaties zoals:

- ISO: International Organization for Standardization
- IEEE: Institute of Electrical and Electronics Engineers
- IEC: International Electrotechnical Commission
- ITU: International Telecommunications Union
- IETF: Internet Engineering Taskforce
- …

Anderzijds zijn er standaarden uitgebracht door industriële consortia zoals:

- BACnet International: BACnet standaard
- KNX Association: KNX standaard
- LonMark International: LonWorks standaard
- DiiA: Digital Illumination Interface Alliance: DALI standaard
- EnOcean Alliance: EnOcean draadloze standaard
- Bluetooth Special Interest Group (SIG): Bluetooth standaard
- Connectivity Standards Alliance: o.a. Zigbee en Matter standaarden
- Thread Group: Thread standaard
- …

Standaarden en open protocollen ontstaan dus door samenwerking tussen verschillende organisaties, waaronder bv. fabrikanten en aanbieders van diensten. Ook organisaties die niet deelnemen aan de ontwikkeling van een standaard en/of open protocol, kunnen beslissen om deze toe te passen in hun producten en diensten. Op die manier ontstaat er een ecosysteem van organisaties die producten en diensten kunnen aanbieden die een grote mate van compatibiliteit en/of interoperabiliteit kennen. Om deze compatibiliteit en/of interoperabiliteit ook te verzekeren, kunnen er onderlinge testsessies ('plugfests') georganiseerd worden tussen organisaties of kan er een test- en certificatie-programma opgezet worden door de organisatie die verantwoordelijk is voor de standaard of het protocol dat in de standaard beschreven wordt.

6.1.2 Gesloten en propriëtaire protocollen

Naast de meer open protocollen en standaarden die tot stand komen via samenwerkingen tussen meerdere organisaties, bestaan er ook eerder **gesloten protocollen**. Deze worden **typisch** ontwikkeld door **een enkel bedrijf** en zijn dan ook **meestal eigendomsmatig of propriëtair**. Het bedrijf (bv. een fabrikant) is dan als eigenaar van het protocol verantwoordelijk voor de ontwikkeling en het beheer ervan. Het gebruik van gesloten protocollen zorgt ervoor dat compatibiliteit beperkt blijft binnen het portfolio van het bedrijf.

Noteer dat ook open protocollen propriëtair kunnen zijn wanneer deze eigendom zijn van en beheerd worden door een industrieel consortium (bv. KNX, DALI).

6.1.3 Open versus gesloten?

Openheid van protocollen is **geen zwart-wit begrip**. Een protocol kan bijvoorbeeld als open gezien worden omdat het als standaard publiek beschikbaar gemaakt wordt. Tegelijkertijd kunnen er aan het gebruik van een (al dan niet gestandaardiseerd) protocol (soms indirecte) kosten verbonden zijn, wat zorgt voor minder toegankelijkheid (en dus meer geslotenheid).

In praktijk wordt vaak een **combinatie van gesloten en open protocollen** gebruikt. Zoals vermeld onderaan pagina 8, voorzien sommige open protocollen de mogelijkheid om gesloten functionaliteit te gebruiken binnen het protocol. Daarnaast beschrijven veel protocollen slechts een gedeelte van de benodigde protocollagen uit het OSI model, waardoor sowieso een combinatie van meerdere protocollen nodig is. Dit kunnen meerdere open protocollen zijn maar kan ook een combinatie van open en gesloten protocollen zijn. Zo maakt Zigbee gebruik van de open protocollen uit de IEEE 802.15.4 standaard voor de onderste lagen uit het OSI-model en kan de applicatielaag in sommige gevallen ingevuld worden via fabrikant-specifieke gesloten profielen. Ook op hoger niveau zijn combinaties mogelijk. Zo kan een systeem voor de interne werking (compatibiliteit tussen componenten) een gesloten protocol gebruiken, maar tegelijk voor een interface een open protocol ondersteunen om zo interoperabiliteit met andere systemen toe te laten.

Zowel gesloten als open protocollen (en standaarden) hebben voor- en nadelen voor de verschillende stakeholders zoals fabrikanten, integratoren en eindgebruikers.

6.1.3.1 Standpunt fabrikant

Vanuit het oogpunt van een fabrikant kan een **gesloten protocol** bijvoorbeeld interessant zijn om snel en autonoom oplossingen te ontwikkelen die voorzien in specifieke functionaliteit toegespitst op specifieke toepassingen. Hierdoor kunnen deze **efficiënter en/of goedkoper** zijn dan oplossingen gebaseerd op standaarden en open protocollen en kan **sneller** ingespeeld worden op een specifieke vraag. Een ander mogelijk voordeel van gesloten protocollen is dat informatie over de werking ervan niet publiek vrijgegeven hoeft te worden en daardoor minder gemakkelijk in handen kan vallen van partijen met slechte bedoelingen (‘**security by obscurity**’). Ook op technisch niveau kunnen gesloten protocollen interessanter zijn. Zo kan een gesloten protocol ontworpen worden om superieure eigenschappen te hebben op gebieden zoals doorvoersnelheid, vertraging (‘latency’), capaciteit, veiligheid, betrouwbaarheid, etc. Tot slot geeft het gebruik van gesloten oplossingen de fabrikant meer mogelijkheid tot **controle over de intellectuele eigendom**.

Standaarden en open protocollen kunnen voor een fabrikant dan weer als voordeel hebben dat er **minder intern onderzoeks- en ontwikkelingswerk** nodig is, zeker wanneer beperkt of niet deelgenomen wordt aan het ontwikkelingsproces binnen de standaardisatieorganisatie. Daarnaast is het dankzij de **grotere interoperabiliteit** binnen een groter ecosysteem met meerdere fabrikanten, niet per se nodig om zelf een volledig ecosysteem aan te kunnen bieden. Een fabrikant zou zich kunnen

concentreren op specifieke componenten of systemen die kunnen interageren met oplossingen van andere fabrikanten binnen het ecosysteem van de standaard of het protocol.

Een ander voordeel van standaarden en open protocollen is dat ze meestal een grondig en goed gedocumenteerd ontwerp-, ontwikkelings- en verbeteringsproces ondergaan, waardoor de componenten, systemen en diensten die er gebruik van maken een **hoge kwaliteit en veiligheid** (bv. elektrisch, cybersecurity, …) kunnen bieden. Publiek beschikbaar maken van informatie over de werking van een protocol laat toe om eventuele kwetsbaarheden sneller te detecteren en te corrigeren ('security by design'). Dit betekent niet dat gesloten protocollen deze eigenschappen niet kunnen bieden, maar gezien de complexiteit van bepaalde thema's kan het soms gemakkelijker zijn om met een standaard of open protocol te werken.

Keerzijde is wel dat de **ontwikkeling en aanpassing** van een standaard typisch **traag** is gezien er consensus tussen heel wat verschillende stakeholders moet gevonden worden. Noteer dat in sommige gevallen standaarden de mogelijkheid voorzien om bepaalde onderdelen gemakkelijker aan te passen zonder de standaard zelf aan te passen. Dit kan bijvoorbeeld door bepaalde parameters of configuraties open te laten voor invulling door een fabrikant. Daarnaast wordt er binnen bepaalde standaarden de mogelijkheid geboden om nieuwe modellen via een relatief snel proces goedgekeurd te krijgen door het standaardisatieorgaan. Deze 'shortcuts' hebben wel meestal wel een negatieve invloed op de interoperabiliteit.

Vanuit strategisch of commercieel standpunt tot slot, kan het voor een fabrikant in bepaalde gevallen interessant zijn om een eigen ecosysteem op te bouwen waarbij compatibiliteit en/of interoperabiliteit met concurrerende oplossingen niet gewenst is. Andere partijen denken dan weer omgekeerd en zien interoperabiliteit en/of compatibiliteit met oplossingen van andere fabrikanten binnen een breder ecosysteem net wel als strategisch of commercieel interessant.

6.1.3.2 Standpunt eindgebruikers

Vanuit het oogpunt van de eindgebruiker kunnen de mogelijke **voordelen** van oplossingen die gebruik maken van **gesloten protocollen** onder andere een **lagere investeringskost** zijn. Toch hoeft het niet altijd zo te zijn dat oplossingen op basis van gesloten protocollen goedkoper zijn. Daarnaast kan het ook als een gemak gezien worden om te kiezen voor een oplossing op basis van gesloten protocollen, uitgaande van een **totaaloplossing** die door een **enkele aanbieder** kan verzorgd worden. Ook hier moet gezegd dat dit niet noodzakelijk anders is bij oplossingen die gebruik maken van open protocollen.

Mogelijke **nadelen** van oplossingen die gebruik maken van **gesloten protocollen** zijn onder andere dat de **compatibiliteit en/of interoperabiliteit** met oplossingen van andere aanbieders **beperkt** is tot de voorziene interfaces (bv. via een gateway of API), het beperkte zicht op de degelijkheid van de oplossing ('**black box**': bv. gebrek aan informatie over werking protocol, ontbreken van controle en/of certificatie door derde partijen) en de risico's die gepaard gaan met lange termijn afhankelijkheid van een enkele organisatie. Dit laatste wordt ook wel eens '**vendor lock-in**' genoemd en omvat onder andere het risico op te hoge operationele kosten, mogelijke problemen met lange termijn ondersteuning en onzekerheid bij faillissement of overname. Door het afsluiten van een contract met lange termijn afspraken kunnen de meeste van deze nadelen ondervangen worden.

Hoge operationele kosten kunnen bijvoorbeeld ontstaan doordat de eindgebruiker voor onderhoud, upgrades of aanpassingen aangewezen is op een enkele aanbieder (bv. fabrikant) of een beperkt aantal aanbieders (bv. door een fabrikant aangestelde/aanvaarde installateurs/integratoren). Lange termijn ondersteuning kan problematisch zijn wanneer het verdienmodel van een aanbieder erin

bestaat om regelmatig nieuwe producten uit te brengen en oude producten slechts beperkt te ondersteunen. Er zijn diverse voorbeelden (ook bij grote bedrijven) van gevallen waarbij een bepaald product niet meer ondersteund werd of geüpdatet werd, uit de markt gehaald werd of dat er geen backward compatibele versies ontwikkeld werden.

Faillissement en overname tot slot, zijn reële risico's die niet mogen onderschat worden. Een faillissement zorgt onder andere voor het wegvallen van ondersteuning. Zelfs bij onafhankelijke opererende systemen (bv. niet afhankelijk van een clouddienst) kan dit grote impact hebben. Bij een overname is de impact afhankelijk van de prioriteiten en strategie van de overnemer, maar ook hier is het bijvoorbeeld mogelijk dat een bepaalde productlijn na de overname niet langer ondersteund wordt. In bepaalde gevallen kan een 'escrow'-regeling interessant zijn om mogelijke nadelige gevolgen te beperken: zo kan code bijvoorbeeld bij een notaris gedeponeerd worden en onder bepaalde op voorhand overeengekomen omstandigheden, vrijgegeven worden.

6.2 Openheid softwareprotocollen en -standaarden

Ook voor de softwaresystemen gebruikt binnen (of boven) gebouwsystemen is openheid belangrijk om interoperabiliteit op applicatieniveau te kunnen bereiken.

Enerzijds is er de software zelf. Softwareprogramma's en websites worden geschreven in een programmeertaal (bv. C, Java, PHP, Python, …) en meestal voor een bepaald besturingssysteem (bv. Linux, Windows, macOS, Android, iOS, …). De programmeertaal en het besturingssysteem kunnen van belang zijn indien aanpassingen of uitbreidingen moeten gebeuren aan de software. Indien de blauwdruk van de software (de 'broncode') vrij ter beschikking gesteld wordt, spreekt men van '**open source**' software. Wanneer dit niet het geval is spreekt men van 'proprietary' software.

Anderzijds zijn er de interfaces die software toelaat te interageren met andere systemen. Deze interfaces verzorgen onder andere de interacties tussen softwareapplicaties onderling (bv. via een API) en interacties tussen softwareapplicaties en gegevensbanken (databases).

Met het oog op interoperabiliteit zijn vooral **open en gestandaardiseerde interfaces** van belang. Het zijn namelijk deze interfaces die samenwerkingen tussen de verschillende interne en externe systemen (bv. cloud-gebaseerd) mogelijk maken.

6.3 Openheid configuratie

De **configuratie van** de **systemen en componenten** binnen een Smart Building is van uitermate belang. Het is immers de configuratie die de **werking van de Smart Building** zal bepalen. Openheid van configuratie is in dat opzicht misschien zelfs belangrijker dan openheid van protocollen. Wanneer de analogie met een auto gemaakt wordt, zou kunnen gesteld worden dat de configuratie gaat over het besturen van de auto, terwijl de protocollen gaan over wat er zich onder de motorkap afspeelt.

De configuratie van een systeem of component kan **verschillende vormen** aannemen afhankelijk van de gebruikte technologie en protocollen. Zo zal de configuratie van een eenvoudige component op veldniveau meestal gelimiteerd zijn tot enkele parameters (bv. adressering) terwijl geavanceerde componenten zoals een centrale controller in een coördinerend systeem een meer complexe configuratie zullen vereisen, bv. in de vorm van tabellen met parameters of softwarecode (bv. scripts).

Complexere vormen van configuratie zoals **softwarecode** bieden uitgebreide **mogelijkheden** maar brengen ook een aantal **risico's** met zich mee. Geschreven softwarecode gaat gepaard met **intellectuele eigendomsrechten** die al dan niet overgedragen kunnen worden. Ook is softwarecode, zeker wanneer deze niet goed gedocumenteerd is, **niet altijd eenvoudig te interpreteren** door iemand

anders dan de programmeur. Eenvoudige vormen van configuratie hebben het voordeel dat ze gemakkelijker aan te leren zijn (bv. aan techniekers) en dat ze meestal ook gemakkelijker te interpreteren zijn achteraf.

Wanneer de configuratie afgeschermd wordt door één partij zoals de fabrikant of integrator kan men van een **gesloten configuratie** of '**vendor/integrator lock-in**' spreken. Hoewel een configuratie beheerd door één partij voordelen kan hebben (bv. één aanspreekpunt met goede kennis van het systeem) dient men waakzaam te zijn voor de mogelijke nadelen die gepaard kunnen gaan met een gesloten configuratie. Zo is het misschien wenselijk om als eigenaar zelf aanpassingen te kunnen maken aan de functionaliteit van het gebouw of moet een derde partij zelfstandig aanpassingen kunnen maken om bijvoorbeeld een bijkomend systeem of toepassing toe te voegen. Dit is vaak niet mogelijk is als de configuratie afgeschermd wordt. Ook wordt, net als bij het gebruik van gesloten protocollen, best rekening gehouden met de risico's die gepaard gaan met het afhankelijk zijn van een enkele organisatie.

Een technische oplossing die de openheid van de configuratie ten goede komt is de zogenaamde **'readback' functionaliteit**. Via deze oplossing kan de bestaande configuratie van een systeem uitgelezen worden. Hierdoor is zelfs bij verlies van eventuele configuratiebestanden de configuratie nog steeds toegankelijk en is het mogelijk om back-ups te nemen en indien nodig een roll-back uit te voeren naar een vorige versie van de configuratie. Protocollen die voor de configuratie van componenten en systemen geen read-back functie toelaten, doen dit dikwijls om de intellectuele rechten van de programmeur te beschermen.

Merk op dat bij het gebruik van meerdere systemen die gebruik maken van verschillende protocollen (bv. BACnet voor het coördinerende gebouwbeheersysteem en DALI voor verlichting), er **meestal afzonderlijke configuraties per systeem** nodig zullen zijn. Het is in dit geval immers niet mogelijk om de configuratie van een onderliggend systeem (bv. verlichting via DALI) uit te voeren via een coördinerend systeem (bv. gebouwbeheer via BACnet). In sommige gevallen kunnen bepaalde gebruikersparameters aangepast worden via een coördinerend systeem , maar de adressering dient steeds per individueel systeem te gebeuren.

7 Organisatorische aspecten

Traditioneel worden gebouwen voorgeschreven via aparte loten voor de verschillende gebouwsystemen, waarbij de coördinerende systemen nodig voor een Smart Building bijvoorbeeld binnen het lot HVAC of elektriciteit worden opgenomen. Dit terwijl deze systemen een veel bredere scope hebben die de silo's overstijgt. Deze manier van werken is een mogelijke bron van problemen voor het bereiken van de nodige interoperabiliteit waardoor het moeilijk kan worden om de gewenste Smart Building functionaliteit te realiseren.

Gezien het belang van interoperabiliteit binnen een Smart Building, is het veelal meer aangewezen om een **apart lot** te voorzien voor **systeemintegratie** (bv. via een GBS of een BOS). Op die manier is er een partij die zich expliciet bezig houdt om alle integratie te voorzien en kan de nodige aandacht besteed worden aan de keuze en implementatie van de coördinerende systemen die voor een groot deel bepalen in welke mate slimme toepassingen zullen kunnen gebruikt worden. Een bijkomend voordeel van het voorzien van een apart lot voor systeemintegratie is dat de partij die hiervoor aangesteld wordt, doorgaans een stuk sneller in het bouwproces betrokken zal worden en er dus ook over kan waken dat beslissingen die genomen worden steeds in lijn liggen met de "geïntegreerde aanpak" en technisch haalbaar zijn. Om het bouwproces optimaal te laten verlopen, is het dus in elk geval interessant om **zo vroeg mogelijk** (bv. tijdens de studiefase) **de nodige partijen** te **betrekken**, o.a.:

- Eigenaar
- Huurder
- Ontwerper
- Studiebureau
- Aannemer/installateur
- Systeemintegrator
- IT-verantwoordelijke
- Gebouwbeheerder
- Gebouwgebruiker
- Onderhoudsbedrijf
- …

Voldoende communicatie tussen de verschillende partijen van bij de start van het project kan ervoor zorgen dat er bij de uiteindelijke keuze van de verschillende technische systemen voldoende rekening gehouden wordt met mogelijke impact op coëxistentie, compatibiliteit, uitwisselbaarheid en interoperabiliteit.

8 Conclusie en aanbevelingen

Coëxistentie, compatibiliteit, uitwisselbaarheid en **interoperabiliteit** zijn **complexe, maar belangrijke concepten** om mee rekening te houden bij het realiseren van een Smart Building. **Openheid**, in elk van de bestaande vormen, **speelt een belangrijke rol** bij het nastreven van deze concepten. **Interoperabiliteit** focust op **interactie op systeemniveau** en is daarom misschien wel de belangrijkste van bovengenoemde concepten. De functionaliteit van een Smart Building steunt immers in grote mate op interacties tussen systemen. De specifieke implementatie van deze systemen kan in dat opzicht als minder belangrijk gezien worden. Er zijn verschillende manieren om de gewenste interoperabiliteit tussen de verschillende systemen te bereiken. Typisch wordt een **bovenliggend coördinerend systeem** voorzien om de interacties tussen de verschillende gebouwsystemen en interacties met externe systemen te faciliteren.

Op technisch niveau, bestaan er vandaag heel wat standaarden en protocollen voor gebouwsystemen die verschillende graden van openheid kennen. **Typisch** zullen er in een gebouw **meerdere standaarden en protocollen (open/gesloten) gebruikt** worden in de verschillende systemen. Open en gesloten protocollen hebben elk hun voor- en nadelen. Een grondige afweging, rekening houdend met de aangebrachte elementen wordt dan ook aanbevolen. Naast **openheid van protocollen**, is ook **openheid van configuratie** een niet te verwaarlozen aandachtpunt.

Binnen het huidige landschap van standaarden en protocollen lijkt er een tendens te zijn om als onderliggende communicatiemedium (OSI laag 1 tot 3) meer en meer gebruik te maken van Ethernet/IP-gebaseerde netwerken (zie bijvoorbeeld initiatieven zoals IP-BLiS en Matter). De cluster verwacht dat ook protocollen die niet gebaseerd zijn op IP (bv. veldbussystemen) een belangrijke rol zullen blijven vervullen en is overtuigd dat de **toekomst** dan ook "**hybride**" zal zijn. **Veldbussystemen** en systemen die werken met traditionele digitale en analoge inputs en outputs zullen belangrijk blijven omwille van de relatief lage kost & complexiteit, grote betrouwbaarheid en lange levensduur. Dergelijke systemen zijn vaak de meest efficiënte oplossing om de vele componenten op veldniveau in een gebouw (verlichting, thermostaten, detectoren, kleppen, sensoren, etc.) te verbinden. **IP-gebaseerde systemen** hebben dan weer als voordeel dat ze over meer (reken)capaciteit beschikken waardoor complexere functionaliteit kan gerealiseerd worden. Bovendien zijn ze ook geschikt voor het realiseren van interoperabiliteit met andere IP-gebaseerde systemen binnen en buiten het gebouw (bv. lokale IT systemen, clouddiensten, ...).

Op organisatorisch niveau, beveelt de cluster aan om zo vroeg mogelijk in het bouwproces een **onafhankelijke verantwoordelijke voor het aspect systeemintegratie** (bv. systeemintegrator) aan te stellen en actief te betrekken. Het is zijn/haar taak om een algemene strategie op te stellen voor de gebouwsystemen en te bepalen hoe deze met elkaar dienen samen te werken. Op die manier kan de (voor een Smart Building noodzakelijke) **geïntegreerde aanpak** verzekerd worden en kan voldoende rekening gehouden worden met de in deze tekst aangebrachte aandachtspunten.

9 Bronnen

(SBA), S. B. (n.d.). *SBA Schema couches interoperabilites R2S*. Retrieved from Smart Building Alliance: https://www.smartbuildingsalliance.org/wp-content/uploads/2019/04/SBA_Schema-couches-interoperabilites-R2S.jpg

Bellec, J. (2019, 02 25). *The Smart Building requires its own Operating System (BOS)!* Retrieved from LinkedIn: https://www.linkedin.com/pulse/smart-building-requires-its-own-operating-system-bos-j%C3%A9r%C3%A9mie-bellec/

Intesis. (2021, 02 16). *Intesis DALI Gateways*. Retrieved from Intesis: https://www.intesis.com/products/protocol-translator/dali-gateways/dali-knx-ibox-knx-dali

ZigBee and WiFi Coexistence. (n.d.). Retrieved from Metageek: https://www.metageek.com/training/resources/zigbee-wifi-coexistence.html