Lichtsturing
Voor de lichtsturing wordt gebruik gemaakt van een draadloos systeem, om naast optimaal energieverbruik aan alle verlichtingseisen voor visueel comfort en visuele prestatie van diverse ruimtes te voldoen.
Met de primaire functionaliteiten:

- Aanwezigheidsdetectie;
- Automatische lichtregeling;

Optionele functionaliteiten die het systeem biedt:

- Het geven van inzicht in gebruik van installaties en ruimtes;
- Data van de sensoren delen met andere systemen;
- Het bieden van een infrastructuur voor de IoT-communicatie in een slim gebouw.

Alle armaturen zijn voorzien van een sensor-node, zijn verbonden met een sensor-node of communiceren draadloos met een sensor-node.
De sensor-nodes communiceren op basis van gedistribueerde intelligentie, elke sensor-node neemt zijn eigen beslissingen en is niet afhankelijk van een controller, hub of gateway voor de lichtregeling.

Elke sensor-node ontvangt en zendt informatie met infrarood communicatie naar nabijgelegen armaturen/ sensor-nodes en wisselen daarmee onderling informatie uit op basis van de geselecteerde persoonlijkheid (optimalisaties voor verschillende toepassingen en besparingspotentieel).
Door de RF-mesh technologie creëren de sensor-nodes een fijnmazig gebouwbreed IoT-netwerk (Smart Builing Infrastructuur) op basis van het Wirepas Mesh protocol, waarbij elke sensor-node zijn data deelt voor optioneel* gebruik in een portal of voor een API en/of BACnet koppeling.

**Voor het delen van data in een portal, zal aanvullend gebruik gemaakt dienen te worden van een IoT-gateway(s), het systeem is hierop voorbereid en modulair uitbreidbaar.*

Het systeem biedt Plug & Play functionaliteit en hoeft niet direct te worden geprogrammeerd bij installatie, aanwezigheidsgegevens worden gedeeld en het lichtniveau past zich automatisch aan op basis van aanwezigheid zonder handmatige interventie.

Voor oplevering zal op basis van de gebruikerswensen de volgende instellingen geconfigureerd dienen te worden:

- Zones: Het groeperen van armaturen zodat ze als een eenheid reageren;

- Persoonlijkheden: Voorgeprogrammeerde instellingen of profielen die bepalen hoe een individueel verlichtingsarmatuur (of een groep armaturen) reageert op zijn omgeving;
- Lichtniveaus: Aanpassen van maximale en minimale lichtniveau en de tijdsduur dat het licht aanblijft na de laatste beweging;
- Daglichtregeling: Functionaliteit inschakelen en kalibreren voor optimalisatie van het energieverbruik bij daglichtintreding;
- Handmatige bediening: Koppelen en configureren van batterij of batterijloze (EnOcean) schakelaars voor handmatig bediening (aan/uit, dimmen & scenes activeren) van de verlichting.

Sensor betrouwbaarheid en security

De licht besturing over Infrarood heeft diverse beveiligingen ingebouwd waarbij de IR boodschap lengte niet langer is dan 40 bits, een beperkte berichtenset en bandbreedte heeft.
De IR berichten die kunnen worden geaccepteerd door het systeem hebben een specifieke string lengte met CRC-controle.
Elk extra bericht zal niet worden geaccepteerd of begrepen en kan het systeem dan ook niet op reageren.
De berichten die de configuratieparameters veranderen of nieuwe automatische operatiemethodes activeren kunnen alleen in het systeem worden gepusht door de bijbehorende mobiele App of wanneer er een Gateway in het systeem wordt geplaatst welke zijn eigen beveiliging heeft.

Cyberaanvallen worden gecategoriseerd als volgt:

- Het stelen van data: Er is geen enkele mogelijkheid data te stelen omdat er geen data opgeslagen wordt. Alle communicatie is in real-time en de aansturing is gebaseerd op peer-to-peer communicatie op basis van aanwezigheid als deze niet is gedetecteerd door de eigen sensor;
- Aansturen van de verlichting: Het bedienen van de verlichting gaat vanaf de EnOcean switch en Mobiele telefoon middels Bluetooth Low Energy beaconing. Er is geen dataverbinding tussen de sensor-node en het bedieningsorgaan;
- Beinvloeden van de configuratie: Is alleen mogelijk met ‘Configurator’ toegang en aanwezigheid in de ruimte waar de verlichting hangt.
  Configuratie gebeurt met een mobiele telefoon middels Bluetooth Low Energy beaconing. Er is geen dataverbinding tussen de sensor-node en het bedieningsorgaan.

Communicatie over de Wirepas Massive Mesh RF

- Het Wirepas Massive Mesh protocol maakt gebruik van end-to-end encryptie en elk netwerk van Wirepas heeft twee 128-bits AES-encryptie sleutels;
- Een netwerk dat Wirepas Massive gebruikt bestaat alleen maar uit nodes met de juiste encryptie sleutels;
- De sensor-nodes zelf zijn sabotagebestendig;
- Uit veiligheidsoogpunt en om de flexibiliteit te waarborgen wordt er geen sensor data opgeslagen in de sensor-node.

Communicatie met en opslag in de optionele cloud portal

- Enterprise-level data beveiliging via encryptie op zowel het transport (128bit AES, TLS) als de opslag (EU Amazon AWS IoT);
- Er is een 2 stappen authenticatie (2FA) vereist voor API-toegang tot de real-time en opgeslagen data in de portal/cloud of men hanteert IP-whitelisting in overleg met de eigenaar van de data.

Certificering

- De fabrikant heeft de ISO 27001 certificering, voldoet aan de norm 180301 en is NIS2 compliant;
- Alle producten voldoen aan de geactualiseerde Radio Equipment Directive (RED) 2014/53/EU, inclusief de verplichte aanvullende eisen conform Gedelegeerde Verordening (EU) 2022/30 (art. 3.3 d, e en f) met betrekking tot cybersecurity en gegevensbescherming (in werking getreden op 1 Augustus 2025).