

L'Editoriale

Ing. Francesco Marinuzzi Ph.D.



Dall'edificio alla Smart City: come garantire la sicurezza nelle nuove soluzioni digitali per la sostenibilità ambientale.

La qualità degli edifici ha un forte impatto in termini di sostenibilità ambientale e di qualità della vita considerando che si passa in essi la maggior parte del tempo. In quest'ottica specifiche normative stanno dotando gli edifici di impianti e sistemi avanzati sia dal punto di vista digitale che energetico.

Il Decreto-legge 133/2014 convertito nella legge 164/2014 (Sblocca Italia) ha già introdotto con l'articolo 135-bis la necessità per gli edifici del cablaggio strutturato identificando nei casi specifici, indicati dalla circolare del Consiglio Nazionale Ingegneri 279/2013 sul DM 37/2008, per la progettazione, gli ingegneri abilitati al settore dell'informazione.

La direttiva europea 2010/31/UE, recepita in Italia dal DL 63/2013 poi tramutato in Legge 90 il 3 agosto 2013 e smi, impone l'obbligo di costruire i nuovi edifici, dal 2019 per quelli pubblici e dal prossimo 2021 per quelli privati, con altissima prestazione energetica (nZEB nearly Zero Energy Buildings).

L'edificio viene sempre più ripensato, alla luce delle suddette novità, sia in termini di autonomia energetica (isolamenti e supporto di nuove fonti energetiche rinnovabili) sia in termini di interattività con lo stesso (domotica) e non solo¹. D'altra parte, l'edificio trae molti dei suoi valori aggiunti dalla sua integrazione e posizione nel suo contesto locale (distretto o quartiere) ed in generale nella sua città.

Mentre a livello energetico si inizia a parlare di eco distretti e soluzioni progettuali che affrontano e risolvono a questo livello i temi energetici, dal punto di vista digitale si dà maggiore enfasi alla città, o meglio, alla creazione di Smart City considerando la velocità sempre maggiore di trasferimento dell'informazione.

Le stesse città, a loro volta, sono inserite in un contesto globale soggetto a profonde trasformazioni. Da una parte i cambiamenti climatici, l'aumento dell'inquinamento ambientale prevalentemente da fonti fossili ed il crescere della pressione antropica soprattutto verso i paesi più benestanti e/o le grandi città, dall'altra la continua e sempre più pervasiva digitalizzazione che sta ridefinendo le problematiche e lo spazio delle soluzioni.

Sta aumentando l'esigenza diffusa di adottare stili di vita sostenibili per il pianeta e i nuovi concetti di

Note

1 Per tutta una serie concreta di misure e soluzioni si segnala il portale Internet <http://www.portale4e.it> promosso dall'ENEA

Life Cycle Assessment e Carbon Footprint si stanno rapidamente diffondendo, orientando le scelte quotidiane di ognuno di noi.

Nelle città, proprio grazie alla progressiva digitalizzazione, testimoniata dalla capillare diffusione dei cellulari e delle telecamere, il numero dei crimini, e soprattutto i tempi di scoperta dei colpevoli, si è ridotto.

Non è detto, però, che la nuova rivoluzione digitale del 5G e dell'IoT (internet of things) che realizzerà entro il 2024 molti degli scenari e dei casi d'uso delle Smart City minimizzi i rischi generali. Indipendentemente dalla discussione in atto sul possibile impatto dei campi elettromagnetici delle nuove reti sull'uomo, il controllo in tempo reale, con latenza quasi nulla, del comportamento degli impianti elettrici ed energetici da parte dei sistemi elettronici ed informatici solleva la necessità di una adeguata progettazione ad opera di un professionista abilitato ai sensi del DM 37/2008 già citato (ingegnere dell'informazione per la quota di sistema informatico/elettronico ed industriale per la quota elettrica) che preveda la sicurezza by design.

Da questo punto di vista è bene ricordare che nel digitale la sicurezza dipende molto dalla conoscenza e/o presenza di una vulnerabilità passata, presente o futura su ogni livello, elemento o strato software componente la soluzione anche se di terzi. Pertanto, la sicurezza è una variabile del tempo e come tale va presidiata e garantita nel tempo dalla stessa professionalità che l'ha progettata. In una soluzione Smart City anche la sicurezza fisica diventa, pertanto, variabile nel tempo.

Inoltre, la progressiva efficienza energetica insieme alla sempre più spinta integrazione dei microprocessori che comporta un drastico crollo dei consumi ed una crescita esponenziale della capacità di calcolo permette ai dispositivi una sempre maggiore miniaturizzazione, autonomia di vita e una possibile ed imprevedibile autonomia comportamentale.

Si pone, pertanto, anche un problema di sostenibilità ambientale in senso digitale delle nuove soluzioni Smart City.

A tal riguardo risulta fondamentale distinguere gli elementi passivi in grado soltanto di generare flussi di dati, pur significativi, verso la nuvola e gli elementi o i punti di ricezione delle elaborazioni sul cloud o da remoto e di attuazione e cambiamento del contesto reale.

Mentre i primi, in una certa misura, possono essere distribuiti e diffusi con livelli di controllo minori volti soltanto a verificare la qualità e l'affidabilità del dato rispetto al suo contesto che altrimenti potrebbe falsare l'elaborazione, i secondi, gli attuatori ricettori da cloud o da remoto, devono assolutamente essere soggetti a forti protocolli di controllo e verifica poiché la sicurezza di ognuno di questi potrebbe falsare la sicurezza dell'intero sistema o meglio organismo.

A tal fine il punto di accesso sicuro deve autenticare in modo forte la fonte dei dati, usare un canale di trasmissione sicuro, un formato dei dati verificabile e prevedere un sistema di tracciamento ed allerta di tutti gli eventi praticamente immodificabili: le tante soluzioni blockchain per IoT o i vari sistemi distribuiti alternativi spesso proposti sono tentativi di soluzione al suddetto problema.

Ad esempio, i molteplici e sempre più potenti e numerosi sensori nell'auto o nell'edificio o nei nostri personali device (cellulare, orologio, etc) diventeranno, sempre più, una fonte di valore che abatterà il costo degli stessi contesti in cui sono inseriti e/o potranno generare ulteriore valore monetizzabile, magari, con specifiche cryptovalute come IOTA che adotta un protocollo più efficiente di quello delle blockchain.

Di contro, invece, sarà un bene, limitare al massimo i punti di acting e ricezione da cloud o da remoto e riservare la loro progettazione e gestione nel tempo ai professionisti abilitati previsti esplicitamente dal Dm 37/2008 e dalla circolare CNI 279/2013 anche per una corretta gestione della catena delle responsabilità ed applicabilità di eventuali assicurazioni a copertura dei possibili ed ingenti danni.

Infine, tutti noi vogliamo percepire i nostri ambienti, come sicuri, certi, il porto a cui o con cui tornare dopo la giornata tempestosa. Pertanto, non potremmo sopportare episodi che mettano in grave rischio la nostra incolumità a seguito di disservizi informatici o, peggio, azioni terroristiche o dolose senza minare fortemente la fiducia nell'adozione delle nuove soluzioni pervasive.

Francesco Marinuzzi Ph.D.
Direttore Editoriale