

STATO DELL'ARTE E PROSPETTIVE
DELL'INNOVAZIONE
NEI SERVIZI PUBBLICI LOCALI

ORANGE book

2022



Indice

CONTESTO	5
1 GREEN AND BLUE ECONOMY	8
1.1 Digitalizzazione e trasformazione digitale.....	10
1.2 Dati e <i>Data Drive Business</i>	10
1.3 Modelli, architetture e tecnologie emergenti	14
1.4 Trend globali e di mercato	16
1.4.1 I-IOT su Infrastrutture Critiche	16
1.4.2 <i>Utility e Broadband Services</i>	16
2 DATA DRIVEN ECONOMY.....	19
2.1 Il valore dei dati	19
2.1.1 Patrimonio fondamentale da proteggere e valorizzare	19
2.1.2 Vantaggio competitivo.....	19
2.1.3 I dati abilitano nuovi tipi di business	19
2.1.4 Dati e “spinta gentile”	21
3 DATA DRIVEN DESIGN	23
3.1 Princìpi generali.....	23
3.1.1 Interoperabilità	23
3.1.2 Progettazione by design	24
3.2 Dati e Applicazioni	25
3.2.1 Disponibilità e fruizione dei dati.....	25
3.2.2 Applicazioni software distribuite	25
3.2.3 <i>Service Assurance</i>	26
3.3 <i>Cybersecurity</i>	27
3.3.1 Un obiettivo strategico per il <i>Cybercrime</i> e la <i>Cyberwar</i>	27
3.3.2 Complessità e rischi	27
3.3.3 <i>Cybersecurity lifecycle</i>	28
3.3.4 <i>Supply Chain Security</i>	30
3.3.5 Sicurezza e Resilienza delle <i>Critical Entities</i> nelle Direttive Europee	31
3.3.6 Agenzia per la Cybersicurezza Nazionale	33
4 LA DIGITAL UTILITY	35
4.1 Un nuovo perimetro di business per la “ <i>Digital Utility</i> ”.....	35
4.2 Le sfide della <i>Digital Utility</i>	36
4.3 Il cliente al centro	37
4.4 Visione digitale e posizionamento	37

5	APPENDICE - CASI D'USO	40
5.1	Sensorizzazione e IoT	40
5.2	Software Defined Network e Utility Digital Network	41
5.3	Sostenibilità e resilienza delle città	42
5.4	Automazione e messa in sicurezza di un impianto per la gestione delle acque reflue	44
	BIBLIOGRAFIA.....	53

CONTESTO

L'*Orange Book* è la monografia realizzata dalla Fondazione *Utilitatis* dedicata allo sviluppo e all'applicazione dell'innovazione tecnologica e della digitalizzazione a supporto dell'uso razionale ed efficiente delle risorse.

Comprendere le interconnessioni tra transizione ecologica e transizione tecnologica è fondamentale per cogliere in pieno le opportunità che il mercato offre e prender parte al passaggio in atto, obbligato, da un'economia di produzione lineare a un'economia circolare.

In questo senso, la filosofia espressa in tutti gli *Orange book* è sempre stato proprio il valore della sinergia tra digitale e ambiente, perché la sostenibilità ha come uno dei principali alleati la tecnologia.

La presente edizione dell'*Orange Book* intende fornire una ricognizione sulle leve tecnologiche strategiche per le *utility* e le *multiutility* per consentire loro di costruire architetture digitali, impostando processi e servizi in modo pragmatico, con tutta la flessibilità, l'efficacia e la sicurezza necessarie.

Come verrà di seguito illustrato, oggi al centro di questi cambiamenti in corso ci sono i dati, gli strumenti per raccogliarli e leggerli in modo strategico, cui si aggiunge un altro asset divenuto di conseguenza fondamentale che è la sicurezza cibernetica.

Il contesto attuale si caratterizza da diversi macro fenomeni insieme:

Crisi pandemica

Nel nostro paese e nel mondo si sta attraversando una stagione post pandemica, con le sue ripercussioni economiche, sociali e ambientali.

In risposta alla crisi causata dal COVID-19 si stanno attivando varie politiche. Una prima risposta strutturale del Governo italiano è il *Piano Nazionale di Ripresa e Resilienza* (PNRR): "Il Piano deve contribuire al raggiungimento degli obiettivi ambientali fissati a livello UE anche attraverso l'uso delle tecnologie digitali più avanzate, la protezione delle risorse idriche e marine, la transizione verso un'economia circolare, la riduzione e il riciclaggio dei rifiuti, la prevenzione dell'inquinamento e la protezione e il ripristino di ecosistemi sani", c'è scritto nella prefazione al PNRR a firma del presidente del Consiglio Mario Draghi.

Obiettivi e politiche di sostenibilità

L'Unione Europea, Stato, Regioni, enti locali, ognuno nell'ambito delle proprie competenze normative, stanno operando tutti per definire il processo di decarbonizzazione nei settori ambientale ed energetico.

L'Italia si è impegnata insieme all'Europa a ridurre le emissioni di anidride carbonica del 55% nel 2030 rispetto ai livelli del 1990, con l'obiettivo dichiarato di arrivare alla completa decarbonizzazione entro il 2050.

Il Parlamento italiano ha recentemente approvato in via definitiva la Proposta di legge che modifica gli articoli 9 e 41 della Costituzione. Nell'articolo 9 ora si afferma che "La Repubblica (...) tutela l'ambiente, la biodiversità e gli ecosistemi, anche nell'interesse delle future generazioni". Nell'articolo 41 adesso si afferma che "L'iniziativa economica privata (...) non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana, alla salute, all'ambiente" e che "la legge determina i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali e ambientali".

Per essere attuati, questi programmi ambiziosi richiedono una serie di scelte coerenti in campo tecnologico, economico e geopolitico insieme.

I dati al centro

Le definizioni dei dati come “il nuovo petrolio”, “il nuovo oro”, o addirittura “il nuovo ossigeno”, fanno riferimento al valore enorme che ha assunto il fatto di conoscere i comportamenti degli utenti (siano essi dipendenti di una multiutility oppure clienti/consumatori). Il valore risiede non semplicemente nel raccogliere e possedere i dati relativi a questi soggetti, ma la capacità di saperli leggere e usare per ottenere una comprensione migliore dei processi, delle persone, di un fenomeno, al fine di prendere decisioni più accurate e quindi migliori.

Dati e ambiente

È vero che ogni operazione che coinvolge la gestione dei dati consuma energia, contribuendo così al riscaldamento globale, ma secondo la *Global e-Sustainability Initiative* (Smarter 2020), l'impatto positivo del digitale sull'ambiente potrebbe essere 7 volte più alto del suo impatto negativo, contribuendo alla riduzione del 20% dei gas serra globali entro il 2030. L'utilizzo del digitale nei processi produttivi infatti aiuta l'analogico non sostituendolo, ma permettendo di fare molto di più con molto meno. Questo comporta l'ottimizzazione delle risorse e un notevole risparmio energetico. Il digitale contribuisce inoltre a sviluppare una visione intersettoriale dei settori energetici e ambientali, funzionale a uno sviluppo efficiente delle infrastrutture.

Dati e sicurezza

Insieme ai dati, è divenuto centrale il concetto di sicurezza: l'Italia nel giugno 2021 ha ridefinito l'Architettura nazionale cibernetica e istituito l'*Agenzia per la Cybersicurezza Nazionale* (ACN) a tutela degli interessi nazionali nel campo della digitalizzazione. Le utility rappresentano un obiettivo dichiarato degli hacker e i *cyber criminal*.

Il fattore tempo

Il debito che le future generazioni erediteranno sarà tanto inferiore quanto migliore sarà il connubio tra il verde delle attività ambientali, della produzione energetica sostenibile e dell'economia circolare, e il blu delle tecnologie digitali. Si dice che nessuna crisi dovrebbe andare sprecata e per questo rimane da considerare una variabile fondamentale per il successo di questo connubio: il fattore tempo.

01

GREEN AND
BLUE
ECONOMY



1 GREEN AND BLUE ECONOMY

I cambiamenti climatici, le tensioni internazionali e le interdipendenze geopolitiche, la sempre maggiore difficoltà nel reperire materie prime, le fibrillazioni dei mercati dell'energia, i problemi generati da inquinamento e rifiuti, la deforestazione e la cementificazione, sono tutti fattori che stanno facendo emergere sempre più la necessità di modificare gli attuali modelli di sviluppo e consumo, passando da un'economia lineare a una circolare e dall'utilizzo di fonti fossili a quelle rinnovabili.

La consapevolezza dell'urgenza di mettere in pratica questi cambiamenti da parte di tutti gli attori coinvolti, dalla società alla politica, dall'impresa alla finanza, ha dato concreta propulsione al cambiamento.

Ecco che sostenibilità, recupero, riciclo, energia "pulita" sono gli elementi centrali di tutti i business plan delle utility operanti sul territorio italiano, in una logica di responsabilità sociale di impresa, che armonizza e orienta la mission aziendale verso il benessere delle comunità locali, migliorando la qualità della vita delle stesse, generando occupazione e stimolando ricerca e innovazione.

Senza dubbio, la sfida della transizione verso un'economia sostenibile rappresenta una grande opportunità di crescita per l'Italia e anche di internazionalizzazione per le utility più strutturate (cfr. Road map punto 9, Orange Book 2014). E in questo l'evoluzione tecnologica e la digitalizzazione hanno un ruolo importante: mettono a disposizione dei diversi soggetti sia i dati da analizzare sia gli strumenti per poter agire efficacemente.

L'Unione Europea si è fatta promotrice sia di indicazioni normative sia di stimoli monetari volti a migliorare le politiche di sostenibilità degli Stati membri.

Per poter cogliere appieno il potenziale di questa transizione è necessario adottare un approccio pragmatico che, focalizzandosi sull'obiettivo reale (e non solo sulla mera monetizzazione a breve termine), metta in campo azioni efficaci nei diversi nodi della catena del valore. La sinergia fra i diversi attori del sistema paese potrà svolgere un ruolo moltiplicatore dei benefici attesi, stimolando economia, impresa, lavoro, università e ricerca.

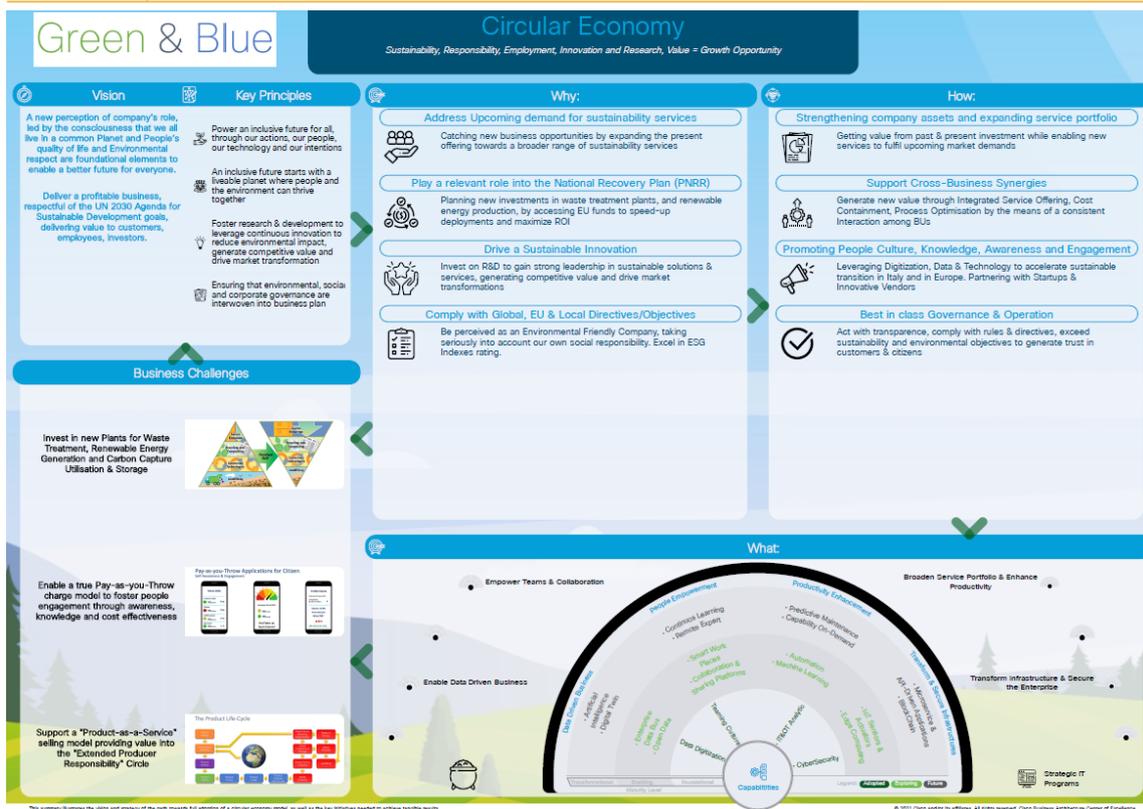
Per l'Italia è certamente un'opportunità unica, in linea con gli obiettivi globali ed europei al 2030 e 2050 (ad esempio l'Agenda 2030 con i suoi 17 obiettivi di sviluppo sostenibile, l'Accordo di Parigi, l'European Green Deal), per accelerare l'adozione di modelli "veramente" sostenibili a livello ambientale e sociale, superando barriere che si sono dimostrate critiche nel recente passato.

Le multiutility giocano un ruolo centrale in questa trasformazione, avendo la possibilità di agire (proprio attraverso la loro mission) direttamente su tutte le componenti cardine della missione 2 del PNRR:

- C1. Economia circolare e agricoltura sostenibile
- C2. Energia rinnovabile, idrogeno, rete e mobilità sostenibile
- C3. Efficienza energetica e riqualificazione degli edifici
- C4 Tutela del territorio e della risorsa idrica

Come suddetto, oggi, e ancor di più nel prossimo futuro, gli obiettivi di sostenibilità vedono nella tecnologia uno dei principali alleati, sotto molteplici punti di vista.

FIGURA 1 | CISCO BUSINESS ARCHITECTURE CENTER OF EXCELLENCE



La sempre crescente digitalizzazione del paese, dei processi produttivi e delle informazioni di contesto, rende disponibile una grande quantità di dati, permettendo di acquisire una migliore conoscenza degli elementi chiave per definire nel modo più appropriato azioni e priorità (*Data Driven Decision Making*).

Nella figura 1 vengono individuate le sfide del settore: in particolare come motivare e abilitare il consumatore e i cittadini, attraverso smartphone, a un loro coinvolgimento nei processi di consumo, facendo leva sulla consapevolezza, conoscenza dei costi ed efficacia dei consumi.

La diffusione della sensoristica IoT (*Internet of Things*) amplia significativamente lo spettro di informazioni su cui poter basare le analisi di contesto, spaziando dalle misurazioni in tempo reale al tracciamento storico dei dati, abilitando quindi un elemento essenziale per il miglioramento della produttività e dell'efficienza operativa: l'automazione.

La disponibilità di reti di comunicazione pervasive, oltre alla raccolta dei dati, permette un migliore coordinamento dei processi, l'accesso ubiquo alle informazioni anche in mobilità, una più ampia collaborazione fra tutti i soggetti coinvolti.

Nella logica Green and Blue, le multiutility saranno chiamate ad ampliare la propria offerta di mercato, divenendo un soggetto di riferimento per la fornitura di **servizi essenziali alla sostenibilità delle aziende e dei territori**. Alcuni di questi possono essere così sintetizzati:

- Mobilità sostenibile (in particolare elettrica)
- Produzione e rivendita di Idrogeno verde da fonti rinnovabili
- Raccolta, recupero e, opzionalmente, trasformazione di prodotti giunti a fine vita, con l'obiettivo di generare materie prime seconde da rivendere alle aziende produttrici (per chiudere la catena della responsabilità estesa del produttore nell'ambito di specifiche categorie merceologiche), generando anche ulteriore valore nel contesto del "product-as-a-service"

- Tariffazione puntuale dei rifiuti, che consenta alle comunità di raggiungere nei tempi previsti gli obiettivi europei del settore, in termini sia quantitativi sia qualitativi

Non da ultimo, data la valenza strategica a livello nazionale dei servizi erogati, è fondamentale che le *multiutility* adottino soluzioni e definiscano politiche di *cyber sicurezza* adeguate e sempre aggiornate rispetto alle minacce emergenti.

1.1 Digitalizzazione e trasformazione digitale

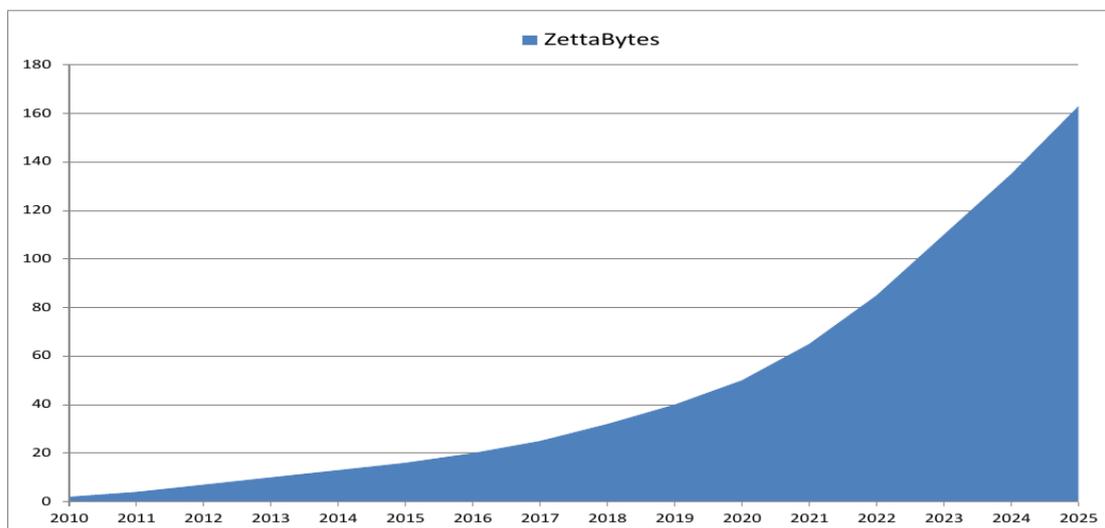
La trasformazione digitale è in generale l'applicazione della digitalizzazione alle aree dell'esistenza e, nel caso del business, ai prodotti, al patrimonio informativo e ai processi aziendali.

I settori in cui si tratta materia prima digitale (software, telecomunicazioni, media, ecc.) hanno fatto della trasformazione digitale un modello di business, mentre gli altri settori ne hanno adottato selettivamente alcune pratiche e modalità di lavoro, spinti da necessità di efficienza, di competizione o di innovazione.

Concentrando l'attenzione sul settore delle utility e delle multiutility, la trasformazione digitale sta avendo un impatto rilevante sui servizi offerti in termini di modalità di erogazione, rendicontazione (chiamata anche *accountability*), gestione e manutenzione, controllo/monitoraggio delle filiere produttive e rapporti con gli stakeholder.

1.2 Dati e Data Drive Business

FIGURA 2 | INDAGINE CONOSCITIVA SUI BIG DATA



Fonte: AGCM, AgCom, Garante privacy.

Sulle basi della digitalizzazione, negli ultimi anni si è assistito a un aumento esponenziale della disponibilità di dati digitali, (figura 2), elemento che richiede alle aziende di sviluppare la capacità di integrare il valore dei *Dati* nel proprio modello di business, anche se il digitale non è il loro prodotto primario, come nel caso delle *utility* del settore ambiente ed energia.

Per sottolineare l'importanza di questo argomento, di seguito ci si riferirà ai “dati” (minuscola) quando si parlerà dell'elemento grezzo e generico (ad esempio: big data), mentre si indicherà con “Dati” (maiuscola, in corsivo) quell'insieme selezionato di dati (smart data), che costituisce il vettore del contenuto informativo, opportunamente gestito e contestualizzato, capace di trasportare e creare valore aggiunto per uno specifico obiettivo.

A tal fine è cruciale il processo di “estrazione di conoscenza” dai Dati, nell'ambito del quale è possibile enucleare, sul piano logico (con possibili ricadute anche su quello giuridico) 3 ordini principali di attività:

- la raccolta, che a sua volta si articola in generazione, acquisizione e memorizzazione;
- l'elaborazione, che coinvolge attività di estrazione, integrazione e analisi;
- l'interpretazione e l'utilizzo (Figura 3).

FIGURA 3 | LA FILIERA DEI DATI



Fonte: AGCM.

Grazie alla distribuzione della capacità di calcolo e alla miniaturizzazione di sensori, attuatori ed elaboratori, e grazie alla pervasività della connettività in rete, nonché alla trasformazione delle interfacce uomo-macchina (piattaforme web, *app* e altro) ora vengono prodotti ed estratti dati in grandissime quantità da oggetti, dall'hardware e software aziendale e dalle interazioni/transazioni digitali che si attuano. Ogni interazione utente è codificata, trasmessa, registrata; ogni elemento fisico può essere potenzialmente comandato e misurato, può quindi produrre nuovi dati, che a loro volta possono essere codificati, trasmessi e registrati.

Si introduce di conseguenza l'espressione *data driven business* (e anche *data driven decision*). Essa rappresenta la capacità delle aziende di integrare i dati nella propria catena del valore, non utilizzandoli più solo come supporto collaterale, ma come parte del business, come strumento di intelligence, come merce di scambio.

Ad esempio, nel contesto dei servizi energetici e ambientali, si pensi alla profilazione degli utenti in base alle loro attività e preferenze, comunicate da loro (in modo esplicito o meno) attraverso l'uso dei siti web o *app*. Gli *smartphone* rivestono un ruolo centrale nell'acquisizione dei dati generati dai clienti, in quanto dispongono di numerosi dispositivi di *input* (come i sensori di movimento, di luminosità, di localizzazione, la tastiera e il *touch screen*) integrati in un unico strumento connesso a Internet, che accompagna il cittadino e il consumatore in tutte le sue attività quotidiane. Va specificato che in uno *smartphone* i veicoli per l'acquisizione dei dati sono rappresentati, da un lato, dal sistema operativo e dall'altro dalle applicazioni pre-installate o successivamente installate dall'utente. Nel secondo caso i dati sono acquisiti dai rispettivi sviluppatori.

Si pensi ai profili di consumo o produzione delle risorse (acqua, energia, gas, rifiuti) e ai dati provenienti dalle reti di distribuzione o logistiche¹. Si pensi inoltre al valore che tutti questi dati possono assumere se scambiati internamente o esternamente nell'ambito dei modelli di organizzazione digitale degli aggregati urbani, quali *smart districts*, *smart cities*, *Smart landscape*, e in genere al contributo delle economie di coordinamento che hanno un beneficio sulle politiche ambientali e climatiche.

È innanzitutto necessario identificare nel modello di gestione dei dati i 5 attributi fondamentali, per definire i *Big Data*, che fungono da guida per la creazione dei processi e degli strumenti dedicati:

- **Volume:** l'effettiva quantità dei dati generati, da produrre, elaborare, trasportare, memorizzare. Questo attributo non solo rappresenta implicitamente la capacità trasmissiva, elaborativa e di memoria dei sistemi adottati, ma anche la necessità di rendere gerarchica la struttura di gestione dei dati;
- **Velocità:** la quantità per unità di tempo dei dati acquisiti, elaborati, replicati. Questo parametro rappresenta un requisito di dimensionamento e progettazione dei sistemi e infrastrutture impattate dal processo di valorizzazione dei dati;
- **Varietà:** la tipologia dei dati è ampia: i dati non sono solo numerici, ma possono assumere nature diverse, come testo, immagini, video, suoni, ecc. Questo implica che gli strumenti di rilevamento (sensori) e gli applicativi di elaborazione devono essere adeguati alla gestione di una base eterogenea per poter abilitare la corretta estrazione e fruizione delle informazioni.
- **Veridicità:** la qualità del dato, frutto dell'accuratezza, affidabilità e "vita utile" dell'informazione. Questo attributo è fondamentale nella gestione del dato in sé, ossia nella modalità in cui viene generato e la tempestività con cui viene portato dalla generazione all'elaborazione, il tempo per cui viene memorizzato e mantenuto disponibile, il peso con cui viene trattato negli algoritmi di elaborazione
- **Valore,** inteso come il contenuto informativo intrinseco del dato, conseguenza della qualità ma anche della contestualizzazione del dato: la misura di quanto il dato è utile agli obiettivi di business prefissati, eventualmente in modo indiretto o combinato con altri dati. In definitiva, il valore regola il ciclo di vita del dato e il modo in cui esso viene utilizzato

La valorizzazione del dato quale *asset* rilevante delle organizzazioni che lo detengono, orienta gli investimenti e l'attenzione verso 2 ulteriori requisiti:

- **Sicurezza: protezione, tutela e resilienza dei dati,** cioè la capacità di creare, elaborare e gestire i dati in modo che non siano trasferiti, modificati o cancellati in modo volontario o involontario, incidentale o fraudolento. La sicurezza del dato, tema di per sé estremamente

¹ Ad esempio dati relativi al dettaglio di microfessure nella tubazione, all'indice di stress di un cavo elettrico, all'usura degli pneumatici di un camion, all'efficienza o allo stato dei siti di stoccaggio o di manutenzione

ampio e complesso, deve permeare ogni fase del ciclo di vita dei dati e deve essere considerata come una caratteristica intrinseca e imprescindibile, dalla loro creazione alla loro eliminazione

- **Privacy:** riservatezza dei dati, che implica la gestione dei processi di CRUD (*Create, Read, Update, Delete*) secondo precisi schemi di autorizzazione e in generale sulla base di una politica basata sulla “necessità di accesso” (*need to access*) del richiedente, unita alla “autorizzazione all’operazione richiesta” (*right to access*) e all’opportuna registrazione dell’accesso e dell’operazione (*log of access*). Di questo tema si occupano in genere normative specifiche, che tuttavia devono essere correttamente calate nei processi e negli strumenti per trovare una soddisfacente realizzazione.

In questo scenario di *Data Driven Business*, il ciclo di vita dell’informazione si sviluppa in 4 momenti temporali:

- **Estrazione:** la fase di acquisizione dei dati da dispositivi di campo (sensori, attuatori, controller, RTU) o da applicazioni che interagiscono con gli utenti;
- **Trasformazione:** passaggio in cui vengono applicate logiche di *business* per filtrare, confrontare, analizzare e codificare il dato grezzo (*raw*) per una pre-elaborazione orientata alla normalizzazione e standardizzazione dello stesso;
- **Governance:** il momento in cui vengono implementate le regole e modalità di accesso ai dati raccolti, in conformità ai principi di sicurezza e privacy;
- **Applicazione:** lo step in cui si disciplina la destinazione dei dati precedentemente elaborati, con particolare attenzione alla creazione dell’informazione e alla presentazione della stessa agli *stakeholder*; in questa fase c’è un forte uso di *analytics* e un lavoro di *business intelligence*.

In estrema sintesi, un *Data Driven Business* è un ecosistema aziendale, che ha al suo interno:

- Le risorse, le infrastrutture e in generale gli asset aziendali
- Le persone e i processi aziendali, inclusa la cultura, le competenze specifiche e la filosofia aziendale
- I clienti o utenti dell’azienda
- I fornitori, i collaboratori e i concorrenti dell’azienda
- I *Dati* prodotti, elaborati e scambiati da tutti gli elementi dell’ecosistema

In tale ecosistema, i *Dati* assumono un valore centrale, e necessitano di processi adeguati a essere trattati e utilizzati per gli scopi prefissi dall’azienda.

L’approccio al tema della centralità dei *Dati* porta con sé diverse conseguenze²:

- Disaccoppia il contenuto informativo dal processo che lo genera, dando la possibilità a varie e diverse realtà aziendali o di ecosistema di valorizzare lo stesso
- Eleva i dati a patrimonio informativo e asset strategico delle utility e del settore in cui operano

² Si può facilmente leggere un parallelismo tra quanto finora accennato e il modello “web 2.0”, ossia quello che ha visto l’integrazione degli utenti nella creazione dei contenuti in rete, da cui sono nati i *social network*. La produzione dei contenuti (i *Dati*) sul “web 1.0”, infatti, era precedentemente appannaggio dei siti web che li rendevano disponibili agli utenti, in una matrice monodirezionale “da pochi a molti”. Con la progressiva e dirompente inversione di tendenza, gli utenti sono diventati produttori di contenuti, integrati nei siti realizzando una matrice “da molti a molti”, facendo crescere esponenzialmente il valore dei siti stessi (o delle *app*) e anche della necessità di avere connessioni a Internet, continue e a banda larga per continuare a creare e consumare contenuti in modo ininterrotto.

- Abilita sistemi di business basati su *data exchange*, punto fondamentale delle missioni 1 e 2 del PNRR

1.3 Modelli, architetture e tecnologie emergenti

Nella costruzione di un *Data Driven Business*, vengono in aiuto modelli e strumenti, che rendono la trasformazione digitale dei processi più agevole.

Il *Data Driven Business* si basa sulla condivisione dei *Dati* all'interno dell'azienda e sulla capacità di gestirne il ciclo di vita, l'accesso sicuro e la disponibilità interna ed esterna secondo le necessità.

In questo approccio, le *utility* possono (e potranno ancora di più nel futuro) sfruttare le potenzialità degli *Open Data*: ossia quei dati a disposizione di tutti, che in ultima analisi consentono di arricchire il contenuto informativo aziendale e e creare un valore aggiuntivo verso l'ecosistema quando esposti verso l'esterno.

Nell'ambito delle tecnologie, numerose soluzioni possono essere individuate a supporto della costruzione di un *Data Driven Business* e della trasformazione digitale dei suoi processi. Riprendendo le fasi del ciclo di vita dei dati come guida, si elencano quelle ritenute più rilevanti:

- 1) **Extract** (*estrazione*): è la fase di acquisizione dei dati da dispositivi di campo e interessa il mondo degli **Apparati Internet of Things (IoT)**, un settore tecnologico già presente da tempo (cfr. Cap 7 *Orange Book 2015*), che permette a grandi linee di digitalizzare la rete di produzione, distribuzione e consumo delle risorse, i macchinari, gli apparati, ecc. (spesso indicato come ambito OT) e di integrarla con la IT per consentire la *trasformazione digitale* attraverso **Reti TLC**, (i.e. 5G, *Low Power Wide Area Range* (es. LORAWAN) e "*Narrow Band IOT*"), **Reti Software Defined-WAN** (o SD-WAN), **Reti di tipo Intent-Based**, e **Protocollo IPv6**. In particolare il protocollo IPv6 sarà l'abilitatore per una reale "rete delle cose" (o Internet of Things). Al momento ammonta a circa il 30% del traffico globale ma è potenzialmente poco considerato nelle applicazioni IoT, anche se già presente in molte di esse. Nel prossimo futuro sarà l'abilitatore delle reti IoT.
- 2) **Transform** (*trasformazione*) il passaggio in cui vengono applicate logiche di business per filtrare, confrontare, analizzare e codificare il dato attraverso **l'Edge o Fog Computing**. In questo passaggio viene resa possibile la capacità di elaborazione degli stessi nodi di rete, funzionali al collegamento degli apparati IT/IoT e la loro capacità di ospitare localmente potenza elaborativa, consente di implementare le gerarchie di elaborazione, riducendo la quantità dei dati trasmessi dalla periferia, consentendo elaborazioni contestuali e risposte/attuazioni tempestive, scambio di dati decentrati senza dipendere da una sola intelligenza centrale. Per poter realizzare le architetture di calcolo distribuite è indispensabile ripensare le modalità di sviluppo applicativo e – in alcuni casi – opportuno pianificare la migrazione di applicazioni esistenti a nuove tecnologie applicative. In questo caso si parla di **MicroService & API-driven application**.
Infine le architetture applicative di nuova generazione, le cosiddette **Hybrid Cloud & Serverless Architecture**: in cui il focus non è sull'operatività dell'infrastruttura ma sulla costruzione e fungibilità dell'applicazione, in accordo con quello a cui ci hanno ormai abituato le applicazioni mobili (semplici, dirette, sempre disponibili, aggiornate, dinamiche e trasversali). Queste ultime notoriamente sfruttano contemporaneamente, e opportunamente, le capacità del *Client* e quelle del *Cloud* in termini di elaborazione e memorizzazione.
- 3) **Govern**: il passaggio fondamentale in cui vengono implementate le regole e modalità di accesso ai dati raccolti, in conformità ai principi della Sicurezza e Privacy che interessano la **Data Science**: legata all'aumento della disponibilità di dati e alla scarsa capacità di governarne la qualità, quantità

e contestualizzazione. In questo contesto per le *utility* è necessario impiegare tecniche e professionisti del settore Data Science (Data Analyst, Data Scientist, ecc.) per realizzare valore non polarizzato dall'insieme di dati disponibili, in modo che sia utile all'azienda e non solo un puro esercizio tecnologico. In questo è necessaria una chiara Data Policy che integri le politiche aziendali e le normative che indirizzano sicurezza e privacy (p.es. GDPR), con gli strumenti tecnologici. Questo ambito è notoriamente cross-aziendale e coinvolge elementi di tutte le strutture, in comitati trasversali che abbracciano tutte le funzioni aziendali e tutti gli ambiti operativi.

- 4) **Dellver:** (*applicazione*) la fase in cui si disciplina la destinazione dei dati precedentemente elaborati con particolare attenzione alla creazione dell'informazione e alla presentazione della stessa ai propri clienti e stakeholder; in questa fase c'è la possibilità di sfruttare le potenzialità degli **analytics** e della **business intelligence**. In particolare raccogliendo dati da ogni area dell'operatività aziendale, che spaziano dagli elementi della rete di distribuzione gas ed energia elettrica, fino a quelli di raccolta e stoccaggio dei rifiuti e dei parametri ambientali diventa possibile incrociare i dati per ottenere informazioni analitiche che abbiano un valore aziendale, o *business value*. Possono essere esempi l'efficienza di conversione di alcune centrali elettriche o idroelettriche, l'usura degli specifici componenti, il livello di riempimento dei cassonetti di raccolta dei rifiuti, il livello dell'acqua nei fiumi o negli impianti di purificazione. I dati non sono però limitati ai soli sensori "quantitativi", ma possono estendersi alle immagini di un gasdotto dalle quali estrarre la presenza di crepe o deformazioni, il suono di una turbina durante l'esercizio, e così via. Da tutti questi dati, eterogenei e complessi è possibile estrarre "trend", tendenze, avvisaglie di guasto, stato dell'infrastruttura. Questi e tanti altri sono esempi di *advanced analytics* che possono essere rese disponibili e creare un "feedback costruttivo" nell'operatività dell'azienda e nell'efficienza, riducendo i costi, aumentando la produttività e la competitività. Sono enormi i progressi fatti negli ultimi anni nell'ambito degli algoritmi di intelligenza artificiale, tanto da consentire una serie di applicazioni "collaborative" in cui entità dello stesso ecosistema possono scambiarsi parametri degli algoritmi e dati sintetici senza per questo condividere dati sensibili su utenti o apparati. Attraverso i dati, gli *analytics*, l'intelligenza artificiale, unitamente ai dati derivati dalle interazioni con i Clienti, con l'ecosistema, con i macro trend locali o globali e le logiche tipiche dell'industria delle *utility* permettono di ottenere un panorama ancor più ampio e profondo di connessione tra i dati, a cui spesso si fa riferimento con il termine "Business Intelligence". Grazie al supporto di specialisti del settore che agiscono o suggeriscono azioni o estraggono contenuti informativi arricchiti, facendo ipotesi, si possono offrire conclusioni o azioni volte al raggiungimento di un determinato obiettivo.

Per quanto riguarda i *Dati*, al di là dell'accezione generica, nell'ambito delle *utility* e *multiutility* si possono indicare 2 aree generali in cui essi ricadono, in base alla loro dinamicità. In questa classificazione si cita anche il processo a cui possono appartenere nell'ambito della struttura aziendale *Data Driven*, per darne una coordinata di riferimento.

Dati statici o scarsamente dinamici

- Dati strutturali/inventariali degli *asset* e della rete di servizio: fanno parte dei dati di base dell'*Asset Management*
- Dati dei clienti: fanno parte dei dati di base del *Customer Management*

Dati dinamici o quasi *real-time*

- Dati dei clienti (interazioni, produzione, consumo di risorse o smaltimento rifiuti): possono essere principalmente utilizzati nell'evoluzione del processo di *Customer Management*, alimentando profili dei clienti, creando profilazioni dell'utilizzo dei prodotti, simulando

domanda/offerta, anticipando *trend* di consumo o generazione, scoprendo andamenti nascosti o a lungo termine attraverso l'uso di algoritmi di intelligenza artificiale.

- Dati di produzione delle risorse (energia, acqua, rifiuti, gas): possono essere principalmente utilizzati rilevando anomalie attraverso strumenti di *analytics*, prevedendo andamenti, pianificando o modificando la domanda sulla base dell'offerta.
- Dati rilevati *real-time/near-real-time* dalla rete di servizio (fattori chiave operativi, manutenzione, attuazione): possono essere principalmente utilizzati rilevando anomalie attraverso gli *analytics*, prevedendo guasti o fermi di produzione, contribuendo ad efficientare il trasporto delle risorse, agendo localmente e in modo automatico in risposta a eventi.
- Dati provenienti da terzi (fornitori/partner/concorrenti, ecc.): possono essere principalmente utilizzati andando principalmente ad alimentare i modelli di gestione domanda/offerta.

1.4 Trend globali e di mercato

1.4.1 I-IOT su Infrastrutture Critiche

Un trend interessante che sta coinvolgendo diverse *utility* a livello nazionale, consiste nella raccolta di nuovi dati che possano essere utilizzati e sfruttati sia dalle stesse aziende, ad esempio nei settori *Oil and Gas*, Distribuzione Acqua ed Elettricità, sia dalle comunità sul territorio.

La capillarità e l'estensione delle reti di questi operatori rendono estremamente preziose queste informazioni soprattutto se pensiamo a un territorio fragile come quello italiano.

Sta quindi emergendo la possibilità di un utilizzo molteplice dei dati: per l'efficientamento e la sicurezza dei processi produttivi e di distribuzione di energia e acqua, per la salvaguardia dei territori interessati, e anche per fornire nuovi servizi anche alle comunità locali.

Pensando all'efficientamento, i sensori *I-IOT* possono svolgere un ruolo essenziale, si pensi ad esempio alle reti del gas naturale o dell'acqua, entrambe soffrono del problema della dispersione di risorsa (*leakage*): tramite i sensori si possono costantemente monitorare le perdite lungo le *pipeline* e predisporre le giuste contromisure.

Con i sensori e con le reti *I-IOT* vengono raccolte in tempo reale informazioni relative a temperature, vibrazioni, presenza di gas nocivi, scosse telluriche, pressioni, anche con *video feeds* (una telecamera ad oggi può svolgere anche il ruolo di sensore rilevando presenza di incendi, persone, animali, oggetti e in generale situazioni critiche) e altro.

1.4.2 Utility e Broadband Services

Un interessante trend osservabile a livello mondiale è quello della trasformazione delle reti delle *utility* in vere e proprie infrastrutture che possano erogare anche servizi *Broadband* ad aziende terze o in collaborazione con i fornitori di servizi del settore (*Internet Services Providers*).

Questo ruolo potrà essere assunto da quelle *utility* che hanno a disposizione un asset prezioso come le fibre ottiche di proprietà (*Dark Fibers*), e che potranno valorizzarne al massimo l'utilizzo grazie alle nuove tecnologie rese disponibili dai rivenditori più affidabili del settore.

La capillarità e la possibilità di coprire zone anche con bassa densità abitativa rendono particolarmente appetibile un tale approccio. Molti *Internet Service Providers* preferiscono invece investire in aree maggiormente dense, rispetto alle zone rurali, a livello di aziende, popolazione e potenziali clienti.

In quest'ottica si osserva sempre più spesso la collaborazione tra aziende *utility* e *Telco providers* e *Internet Service Providers* classici.

Anche in questo caso l'innovazione tecnologica gioca un ruolo essenziale con la possibilità di avere a disposizione altissime bande (400-800 Gbit/sec) con una grande capacità di separazione ed efficientamento dei servizi tramite DWDM e *Routed Optical Network*.

Entrambe le soluzioni permettono di sfruttare al meglio un *asset* prezioso come le fibre ottiche, garantendo l'erogazione multi-servizio in maniera sicura e con grandi livelli di qualità.

02

DATA DRIVEN ECONOMY



2 DATA DRIVEN ECONOMY

2.1 Il valore dei dati

“Se non si può misurare qualcosa, non si può migliorarla”. (Lord William Thomson Kelvin)

2.1.1 Patrimonio fondamentale da proteggere e valorizzare

Un sistema informativo aziendale può essere immaginato come un insieme che comprende persone, funzioni, applicazioni, reti tecnologiche e procedure che, interagendo tra di loro, hanno come obiettivo finale quello di rendere disponibile a un soggetto una serie di informazioni e dati nel momento e nel luogo desiderati. Un sistema informativo è in grado di fare ciò compiendo delle operazioni come ad esempio: raccogliere dati, elaborarli, scambiarli, catalogarli ed esporli, e quindi restituirli sotto forma di informazioni utili al soggetto interessato. Le informazioni finali quindi costituiscono un valore superiore ai dati grezzi, perché sono il prodotto di elaborazioni e aggregazioni di dati con l'intervento di una intelligenza umana o artificiale.

2.1.2 Vantaggio competitivo

Le informazioni fornite dal sistema informativo agli organi aziendali sono necessarie agli stessi per assumere le decisioni, e il loro valore è costituito da:

- Contenuto, ossia la rilevanza per il destinatario e la correttezza intrinseca;
- Tempo nel quale sono rese disponibili;
- Luogo dove sono rese disponibili;
- Forma con la quale sono presentate.

Spesso aziende partner o enti pubblici si scambiano dati e informazioni tra loro per un vantaggio comune: questo richiede la definizione di protocolli e processi che garantiscano la sicurezza, la qualità e la tempestività dei dati.

In un ambiente dinamico e competitivo come quello attuale, le imprese si trovano in una situazione di grande complessità gestionale e hanno l'esigenza di gestire quantità sempre maggiori di informazioni in modo sempre più efficace, efficiente e tempestivo per poter rispondere ai continui cambiamenti del mercato e delle sue esigenze: prendere decisioni velocemente richiede la possibilità di disporre di tutte le informazioni necessarie in tempi rapidi, il che è possibile solo se l'impresa è dotata di un sistema informativo in grado di rendere disponibili le informazioni in tempo reale e in modo strutturato (cruscotti decisionali e *dashboard*).

2.1.3 I dati abilitano nuovi tipi di business

Le tecnologie informatiche offrono grandi potenzialità poiché consentono alle aziende di controllare, pianificare e gestire in modo integrato tutte le attività, nonché di elaborare velocemente una maggiore quantità di dati e informazioni di quanto fosse possibile in passato.

Un esempio tipico è costituito da *Nike*, azienda leader mondiale che si occupa della progettazione, produzione e commercializzazione di calzature sportive, capi d'abbigliamento, attrezzature, accessori e servizi nell'ambito dello sport. Da questo filone principale, *Nike* ha sviluppato attività collaterali basate sull'acquisizione e l'elaborazione dei dati, e che contribuiscono in modo rilevante al fatturato: *Nike* non

solo sfrutta efficacemente i dati per ottimizzare il marketing, la logistica e la produzione, come fanno molte altre aziende, ma commercializzando i dati stessi.

“Prima gli atleti, poi le scarpe”: questo è il mantra delle strategie marketing di *Nike* ed è stato questo modo di pensare che ha spinto la società, nel 2006, a lanciare sul mercato il suo primo *gadget high tech* di massa, ovvero il *Nike + iPod Sports Kit*. È stata una mossa azzardata, concepita per differenziare una volta per tutte la società dalle concorrenti: il *focus* nei dispositivi digitali, ancora una volta, e ancora più del solito, era più sugli atleti (intesi come i consumatori) che sulle scarpe. Il *kit* permetteva di misurare la distanza e la velocità della corsa.

Il lato curioso della faccenda, però, è che sì, il prodotto era in tutto e per tutto *Nike*, ma di fatto tutto quanto era fatto dall'*iPod*. Dal canto suo, *Nike* si era limitata ad avere l'idea giusta e a vendere un *chip* da inserire nelle scarpe e un dispositivo per la connessione *wireless*.

Insomma, quella intrapresa da *Nike* in questo caso con *Apple* può essere considerata come la migliore delle partnership possibili. Nel tempo, *upgrade* dopo *upgrade*, i dispositivi *Nike +* sono migliorati, rinunciando prima all'*iPod* e quindi al *chip*: nel 2010 tutto quanto fu sostituito da un'app per *iPhone*, collegata a una *community* virtuale di oltre 6 milioni di persone che potevano analizzare e condividere i rispettivi traguardi sportivi.

In questo modo, collateralmente, *Nike* ha potuto avvicinarsi maggiormente ai propri clienti, cogliendo l'opportunità di poterli studiare da vicino e di comunicare frequentemente con loro. Questo balzo tecnologico, istituendo de facto un rapporto continuo con il consumatore, permise anche di tagliare del 40% le spese di *advertising*, senza compromettere in alcun modo i numeri delle vendite.

Il tassello finale della strategia marketing di *Nike* di progressivo avvicinamento al cliente è costituito da braccialetto *FuelBand*, che calcola l'energia e quindi – approssimativamente – le calorie bruciate durante il giorno. Per rendere più affidabili i dati rilevati dal braccialetto, *Nike* ha creato una piattaforma online attraverso la quale i clienti possono paragonare i propri consumi di energia. Anche qui, dunque, l'atleta al centro, il prodotto al margine, e il *brand* sempre pronto a motivare maggiormente i propri consumatori/atleti.

Inoltre, tutti questi dispositivi forniscono dati sulla posizione del cliente durante l'utilizzo. È facile immaginare il valore del tracciamento, anche anonimo e solo quantitativo, dei percorsi delle persone che si allenano correndo a *Central Park* nell'ipotesi in cui si voglia determinare la posizione più vantaggiosa di un cartello pubblicitario o di un chiosco per le bibite.

L'importanza attribuita da *Nike* alla gestione dei dati emerge anche dal loro sito di *job posting*, dove si legge:

“Siamo un team di strateghi e scienziati. Una squadra che si pone delle domande e interpreta le risposte. Siamo designer e innovatori. Grandi pensatori ed entusiasti dei dettagli. Siamo domatori di dati e creatori di idee. Il team *Data and Analytics* di *Nike* trasforma i *big data* in strumenti a sostegno dei processi decisionali fruibili dall'azienda. Tramite la scienza della personalizzazione, sfruttiamo intelligenza artificiale e apprendimento automatico per raccogliere, integrare e trasformare i dati in formati utili per fare di più e meglio. Insieme, abbiniamo la scienza dell'analisi dei dati con l'arte delle competenze funzionali per sostenere *Nike* nel raggiungimento degli obiettivi aziendali”.

2.1.4 Dati e “spinta gentile”

I dati possono abilitare le teorie dell'economia comportamentale attraverso la cosiddetta “spinta gentile” o *nudge*, che si attua in forma di azioni, parole, oggetti in grado di spingere, senza imposizioni, le persone verso comportamenti positivi. Un progetto del GSE (Gestore dei Servizi Energetici) ha voluto sperimentare l'approccio offerto dall'economia comportamentale basato sui dati. È stato selezionato un campione di 477 impianti fotovoltaici, di analoga tipologia (tra i 3 e i 20 kW relativi al settore domestico) e nella medesima area geografica (Nord Italia).

Una comunicazione speciale, *nudging*, ha voluto incoraggiare i proprietari dei piccoli impianti fotovoltaici a mantenerli correttamente per aumentarne la producibilità, allo scopo di valorizzare appieno l'investimento fatto.

Gli impianti sono stati suddivisi in 3 gruppi, ciascuno composto da 159 impianti: un gruppo di controllo, che non ha ricevuto alcuna comunicazione, e altri 2 gruppi ai quali sono state inviate le 2 forme di comunicazione *nudging* ormai consolidate nelle scienze comportamentali: il confronto sociale, dove la *performance* del proprio impianto è paragonata a quella di impianti simili, e l'avversione alle perdite, dove si viene informati della perdita in termini di incentivazione monetaria dovuta alla mediocre *performance* del proprio impianto.

Entrambe le comunicazioni *nudging* hanno informato i destinatari delle basse prestazioni dei propri impianti, inducendoli a porre in essere semplici azioni oppure a chiamare un tecnico per aumentarne le *performance*. A tal fine è stata inoltre predisposta un'apposita pagina che riportava i consigli per mantenere al meglio l'impianto.

Gli esiti dell'esperimento hanno dimostrato l'efficacia dell'approccio: nei primi 9 mesi di sperimentazione, a parità di insolazione, gli impianti che hanno ricevuto il *nudge* hanno prodotto mediamente il 4% in più rispetto al gruppo di controllo a cui non era stata inviata alcuna comunicazione. Non solo, il 50% dei destinatari del *nudge* a ridosso dell'invio della comunicazione ha visitato la pagina *web* dedicata attestando, così, la capacità del *nudge* di attivare immediatamente i soggetti.

03

DATA DRIVEN DESIGN



3 DATA DRIVEN DESIGN

3.1 Principi generali

Quando si parla di *Data Driven Design* si fa riferimento a un tipo di progettazione basato sulla raccolta di informazioni quantitative e qualitative volta a supportare le decisioni, si parla quindi di una progettazione a supporto di un *Data Driven Business*.

3.1.1 Interoperabilità

Uno dei fattori fondamentali nell'affrontare un *Data Driven Design* è la capacità di sfruttare quanto più possibile il valore dei *Dati*. Quando il trattamento dei dati diviene centrale, assume altrettanta importanza la possibilità di condividere i dati tra le applicazioni interne ed esterne, rendendole interoperabili per definizione.

L'interoperabilità dei dati è un tema presente anche nel PNRR (progetto 1.3) ma in generale è la prima delle pratiche tra quelle fondamentali, e si applica non solo ai *Dati* vivi dell'azienda, ossia quelli legati al business e al valore che esso veicola, ma anche ai dati strumentali che le infrastrutture si scambiano.

Anche in questo caso, sono da favorire quegli elementi *hardware* e *software* predisposti a comunicare attraverso protocolli *standard*. Si noti che protocolli di rappresentazione dei dati *standard* non implicano necessariamente modalità di trasferimento *standard*, ma solo la capacità di usare una rappresentazione *standard* del dato quando opportuno o funzionale (ad esempio salvando la configurazione del *software* o trasponendo su disco la tabella del Data Base). Questo a sua volta significa basare le proprie scelte di *design* su *standard* di modellazione e rappresentazione dei dati condivisi e consolidati quali YANG, XML, JSON.

L'interoperabilità dei sistemi rappresenta l'aspetto attuativo che completa l'interoperabilità dei dati. È piuttosto naturale difatti collegare la capacità di interoperare a quella tecnologica di utilizzare API (*Application Programming Interface*) che in modo programmatico consentono non solo di trasferire dati, ma anche di eseguire operazioni sugli stessi e addirittura controllare il comportamento di *hardware* e *software*, integrandolo con il resto dei componenti delle architetture di sistemi, applicazioni, basi di dati. Risulta quindi ancora più cruciale nel *design* delle proprie attività costruire e prediligere soluzioni che esponcano e utilizzino API per la gestione dei dati e delle proprie funzionalità. In tal modo sarà sempre possibile far evolvere i sistemi e le applicazioni inserendo nuovi elementi, o mantenere in qualche modo "retrocompatibili" le nuove soluzioni utilizzando API per comunicazione e integrazione.

L'interoperabilità dei protocolli fa riferimento soprattutto all'infrastruttura IT e OT. Mentre nell'IT l'interoperabilità dei protocolli è largamente guidata da *standard* di mercato (ad esempio *Ethernet* e IPv4 per le reti), nel mondo OT questa interoperabilità passa in gran parte per nodi di traduzione e trasduzione, quando disponibili e pratici, che rendono possibile l'interazione tra ambienti eterogenei. Ovviamente quest'ultima non è una situazione ideale, perché genera costi e complessità spesso inefficienti e a volte insormontabili, ma è una situazione in lenta evoluzione verso l'armonizzazione dei protocolli, prerequisito per un vero *Data Driven Business*. In questo campo, si suggerisce quindi di prevedere sin da subito la riduzione quanto più possibile di protocolli proprietari o poco diffusi, prevedere nel *design* di operazioni e processi l'introduzione di nodi di interoperabilità, tradurre i protocolli più vicino possibile alla sorgente, se non fosse praticabile standardizzarli.

3.1.2 Progettazione by design

La continua evoluzione degli *standard* qualitativi, guidata principalmente dalle esigenze di ripetibilità, competitività e industrializzazione, ha portato nel tempo alla creazione di pratiche che si pongono come riferimento della creazione e conduzione di qualsiasi parte costituente il *business*. In alcuni casi, queste *best practice* si sono concretizzate in *standard* più o meno formali, come le note certificazioni ISO che attestano rispondenza di alcune componenti aziendali a certi livelli di qualità.

Il riferimento a *standard* qualitativi è ancora più opportuno nel caso di un *Data Driven Business*, in cui la digitalizzazione diffusa richiede metodologie rigorose, soprattutto alla luce dei nuovi aspetti da essa introdotti. La digitalizzazione, come già accennato, introduce infatti la necessità di permeare tutti i processi aziendali, e quella di trattare i dati secondo metodi che ne garantiscano tutte le caratteristiche di valore già indicate.

Si introduce quindi la dicitura *progettazione by design*, con cui si indica la capacità di disegnare e costruire già dalle prime fasi, processi, dati, strumenti e infrastrutture secondo principi “nativamente” indirizzati di volta in volta a realizzare, limitare o amplificare specifiche caratteristiche o qualità. Un esempio diretto è la costruzione di processi già allineati e certificabili secondo *standard* di qualità industriali, piuttosto che l’adattamento successivo agli stessi *standard*. Un altro esempio, spesso sottovalutato, è il principio della *security by design*, ossia la pratica di integrare in ogni elemento una nativa qualità di sicurezza, per proteggere di volta in volta persone, processi, dati. Applicare il principio di *progettazione by design* significa quindi tenere conto di tutti gli aspetti fondamentali della vita utile di quanto si sta creando o operando, e indirizzarli già nella selezione degli elementi costitutivi, nella loro combinazione e nella loro gestione.

Per esempio, la *sicurezza by design* delle infrastrutture tecnologiche significa adottare processi che tengano conto di possibili errori o violazioni, volontarie o involontarie, in modo da prevederne e mitigarne gli effetti. Spesso questo passa già dalla selezione di *hardware* o *software* che presentino caratteristiche integrate di sicurezza e protezione, quali l’uso di protocolli di cifratura, la rilevazione delle anomalie di comportamento, la capacità di autenticare l’*hardware* o il *software* in esecuzione per assicurarsi che siano legittimi e non modificati. Sulla base di elementi ricchi di funzionalità utili, si applicano poi principi di progettazione che indirizzino la resilienza, l’alta affidabilità, la disponibilità anche a fronte di guasti o anomalie.

Specializzando ancor di più l’esempio della *sicurezza by design*, e calandolo nel mondo delle reti TLC, questo significa che ogni nodo di comunicazione deve proteggere la propria integrità (resistere ad attacchi che ne vogliano modificare *hardware* o *software*, supportare modalità avanzate di autenticazione e autorizzazione delle operazioni svolte sul nodo), quella dei dati in transito (implementando tecniche e protocolli di cifratura o integrità del dato, a tutti i livelli), quella della soluzione di cui fa parte (comunicando dati di telemetria che consentano di avere una visione di insieme, rilevando non solo lo stato del nodo dall’esterno, ma fornendo ad applicazioni di gestione di correlare i dati tra diversi nodi e parti della rete per rilevare anomalie sistemiche, quali un virus informatico in via di diffusione). Inoltre, la progettazione della rete stessa deve tenere conto della possibilità che alcuni nodi vengano a mancare o si comportino in modo imprevisto, che siano soggetti a *bug* (errori) o a *failure* (guasti). La progettazione di una rete deve prevedere quindi, oltre alla sicurezza, anche resilienza e alta affidabilità *by design*, e questo è abilitato sia dalla funzionalità dei nodi che dalle modalità di costruzione e configurazione della rete. Per aggiungere un ulteriore strumento, si pensi alle capacità di automazione: queste consentono di progettare *by design* una rete che oltre a proteggersi passivamente, “guarisca attivamente”, sia nel caso di attacchi informatici che di guasti, operando modifiche automatiche o semi automatiche sulla base di un insieme di direttive e di intelligenza artificiale.

Risulta quindi chiaro da quanto appena descritto, che la *progettazione by design* – applicata non solo agli elementi tecnologici ma a tutti gli aspetti del *business* – è una nuova o rinnovata necessità del *Data Driven Business* e deve far parte degli strumenti base di qualsiasi Azienda moderna del mondo digitale.

3.2 Dati e Applicazioni

3.2.1 Disponibilità e fruizione dei dati

A seconda del settore di attività, le aziende si trovano a gestire diversi tipi di dati di *business* e di dati operativi, tenendo comunque presente che i secondi possono sempre generare nuove iniziative di *business*, come nel caso di *Nike* precedentemente descritto. Generalmente esistono diversi sistemi aziendali, separati per tipo di dato o per linea di business, anche se recentemente c'è stato un grosso impulso nella raccolta e nell'analisi dei dati con la nascita di nuove figure professionali e lo sviluppo di tecnologie come *Artificial Intelligence* e *Machine Learning*.

In ogni caso i *Data Lake* (luoghi destinati all'archiviazione, analisi e correlazione di dati strutturati e non strutturati) e qualsiasi altra base dati non vengono esposti direttamente agli utilizzatori, ma vengono predisposte applicazioni software che ne proteggono l'integrità e la sicurezza, rendendone anche più facile il consumo. Le interfacce utente, sia che utilizzino dati propri o di terze parti, utilizzano punti di accesso controllato ai dati, che vengono esposti sotto forma di API (*Application Programming Interface*). In questi punti vengono applicate le *policy* di controllo degli accessi, sicurezza, *audit*, *billing*, etc.

3.2.2 Applicazioni software distribuite

Il *software* non viene più sviluppato con architetture monolitiche, o semplicemente *client-server*, ormai si sono affermate architetture estremamente distribuite con componenti che girano nel *Data Center*, nel *Cloud*, nei dispositivi personali degli utilizzatori e in luoghi non presidiati dall'IT. Il concetto di microservizio (funzionalità elementare, con un ciclo di vita indipendente, che viene aggregata insieme ad altre per costruire un'applicazione complessa) si accompagna alla possibilità di *deployment* in ambienti ibridi.

Un tipo specializzato di microservizio è quello che fornisce l'accesso ai dati (a un dato elementare oppure a dati aggregati per uno specifico uso). Altri microservizi consumeranno questi dati senza che i loro sviluppatori debbano occuparsi di come il *database* è strutturato, quali sono le logiche di accesso e di sicurezza: tutti questi aspetti sono incapsulati nel servizio che offre il dato. In questo modo gli sviluppatori possono concentrarsi sulla logica di *business* e gli aspetti funzionali dei servizi, invece che sui meccanismi di gestione della comunicazione, di sicurezza, di scalabilità, etc.

Tuttavia, la qualità e la sicurezza della comunicazione sono le preoccupazioni principali di chi deve garantire il servizio di *business*, perché la competizione in qualsiasi mercato si basa ormai in gran parte sull'offerta di servizi digitali.

È quindi fondamentale controllare e governare il sistema per garantire la soddisfazione dei consumatori e di tutti i sistemi interconnessi che supportano il business.

3.2.3 Service Assurance

Secondo il 57% degli utenti, le aziende hanno una sola opportunità per far colpo su di loro, e se il servizio digitale non funziona, non lo useranno più. Secondo l'ultimo report *App Attention Index* rilasciato da *Cisco AppDynamics*, il numero di persone che utilizzano applicazioni e servizi digitali è cresciuto dall'inizio della pandemia da COVID-19. Lo studio globale, che ha analizzato i comportamenti digitali di oltre 13.000 consumatori, ha inoltre riscontrato che le persone non tollerano un'esperienza deludente con le applicazioni utilizzate e che, quando ciò avviene, incolpano l'azienda o l'applicazione stessa, indipendentemente dal tipo di disservizio.

Dall'inizio del 2020, le persone hanno vissuto un'improvvisa e totale dipendenza dai servizi digitali, modificando il modo in cui si relazionano con le aziende, fruiscono di beni e servizi e prendono le decisioni di acquisto. Lo studio mostra infatti che gli intervistati oggi utilizzano il 30 per cento in più di applicazioni rispetto a prima della pandemia. La ricerca evidenzia che, a seguito del loro crescente bisogno e utilizzo di servizi digitali, per il 76% delle persone intervistate, le aspettative nei confronti dei servizi digitali sono aumentate dall'inizio del 2020.

Ciò che è allarmante per le aziende è che, quando tali aspettative non vengono soddisfatte, il 60% incolpa automaticamente l'applicazione e il *brand*, indipendentemente dal disservizio. Che il problema dipenda dall'applicazione - ad esempio pagine che si caricano lentamente, tempi di inattività o problemi di sicurezza - piuttosto che da altri fattori indipendenti, come la scarsa connessione a Internet, *gateway* di pagamento lenti o problemi tecnici con servizi di terze parti, per il consumatore non c'è distinzione e la responsabilità ricade sulla reputazione e sulla percezione del *brand*.

Il 72% delle persone intervistate ritiene che sia responsabilità del *brand* garantire che un'applicazione o un servizio digitale funzionino perfettamente.

Il 92% si aspetta servizi digitali con prestazioni impeccabili e costanti. La fedeltà del consumatore va alle aziende che investono nell'esperienza fornita dalle applicazioni.

Secondo il 57% delle persone, la maggior parte dei problemi riscontrati nell'utilizzo dei servizi digitali potrebbero essere evitati. "Le applicazioni sono diventate un'ancora di salvezza verso la normalità e le persone non sono più disposte ad accontentarsi, vogliono un'esperienza digitale perfetta", ha commentato Linda Tong, vice presidente e direttore generale di *Cisco AppDynamics*. "Oggi più che mai, chi si occupa di tecnologia è sotto pressione nel tentativo di offrire agli utenti la miglior esperienza possibile alla prima interazione".

Il 73% delle persone intervistate dichiara che continuerà ad utilizzare i servizi digitali di cui ha usufruito durante la pandemia, anche quando si tornerà alla normalità. Ciò significa che la pressione a cui sono sottoposte le aziende tecnologiche nell'affrontare la complessità delle moderne architetture per fornire esperienze digitali impeccabili, non scomparirà a breve.

Tradizionalmente, le aziende si sono organizzate per garantire la qualità dei servizi offerti attraverso organizzazioni dedicate all'esercizio delle applicazioni software e delle infrastrutture IT. Team dedicati al monitoraggio, usando soluzioni commerciali o costruite in casa, hanno cercato di intercettare ogni disservizio e di risolverlo nel più breve tempo possibile.

Ormai questo approccio reattivo non è più sufficiente: è necessario anticipare i problemi, evitare che diventino visibili agli utenti impattando la loro fruizione del servizio e di conseguenza il business e la reputazione dell'azienda. Bisogna garantire la disponibilità e le prestazioni e al tempo stesso l'efficienza complessiva del sistema (che consiste nel non allocare risorse in eccesso, generando costi non giustificati, e fare in modo che ogni applicazione abbia sempre a disposizione le risorse di cui ha bisogno

nel momento giusto). Esempi eclatanti sono stati i blocchi, o i forti rallentamenti, di interi sistemi durante i famosi *click-day*. La mancanza di una strategia (e di una soluzione tecnologica) per soddisfare una forte variazione del carico sui sistemi ha prodotto disservizi e reazioni negative, con conseguenti danni di immagine e impatti sul fatturato.

Diventa quindi imprescindibile costruire un'architettura e un modello operativo tali da poter reagire immediatamente, possibilmente prevedendo gli eventi, a qualsiasi problema che possa produrre un disservizio o una penalizzazione delle performance.

Bisogna tenere in considerazione il comportamento delle applicazioni software, dell'infrastruttura e dei servizi di terze parti che il sistema utilizza.

3.3 Cybersecurity

3.3.1 Un obiettivo strategico per il Cybercrime e la Cyberwar

Negli ultimi anni si è assistito a un notevole aumento nel numero di cyberattacchi ai sistemi di controllo delle *utility*, in parte facilitato dall'emergenza COVID che ha visto nel telelavoro l'unico mezzo per assicurare la continuità operativa di molti servizi essenziali e di infrastrutture critiche.

Sono noti alle cronache diversi episodi, dall'ormai classico attacco *ransomware* alla Colonial Pipeline, la più grande rete di oleodotti degli Stati Uniti (maggio 2021) e ai datacenter di ENEL (giugno 2019 e 2020), al tentato avvelenamento delle acque dell'Acquedotto di Oldsmar in Florida (febbraio 2021), fino ai più drammatici atti di *cyberwar* rappresentati dall'incidente industriale innescato in un impianto petrolchimico saudita (agosto 2017) dal *malware injection*, che ha causato il blocco della rete elettrica ucraina (2015/2016) e dal *malware Stuxnet* utilizzato per sabotare la centrale nucleare di Natanz in Iran, (2007-2010).

È chiaro quindi che le *utility* rappresentano un obiettivo dichiarato degli hacker e strategico per i *cyber criminal* sponsorizzati da Stati sovrani e da organizzazioni terroristiche: un cyberattacco a una di esse non solo può impattare sulla produzione e determinare danni all'ambiente e alle persone, ma può anche causare un effetto di interruzioni a cascata delle attività di altri settori vitali: trasporti, telecomunicazioni, sanità, finanza e difesa.

3.3.2 Complessità e rischi

Come spiegato nei capitoli precedenti, l'integrazione tra IT e OT si traduce in un'infrastruttura *cyber-fisica* e una *data fabric* che estendono la visibilità, i controlli e la quantità di dati che le *smart utility* possono utilizzare per essere più efficienti e competitive sul mercato globale. Ma, allo stesso tempo, questa integrazione aumenta i rischi e la superficie di attacco che gli hacker possono utilizzare per infiltrarsi e rubare proprietà intellettuali (IP) o bloccare funzionalità e servizi.

Una fonte di rischi primaria è rappresentata dal fatto che i dispositivi OT, come i sistemi di automazione e controllo industriale (IACS), PLC, DCS, HMI e SCADA, sono basati su apparecchi obsoleti (*legacy*) che, in generale, non presentano funzionalità di sicurezza. Molti modelli infatti non sono gestibili da remoto, il loro software non è aggiornabile per rimediare ad eventuali vulnerabilità e molti apparati sono costruiti utilizzando sistemi *standard* importati da altri sistemi (*embedded*) e con software commerciale di serie (*off-the-shelf*).

La ramificazione di questa infrastruttura integrata IT/OT crea valore perché si estende a tutte le reti di comunicazione aziendale, alle aziende dell'ecosistema, sfrutta i vantaggi dei servizi *cloud* e rende visibili al *management*, in tempo reale, dati e informazioni provenienti dai dispositivi di campo, sensori e contatori intelligenti, installati in luoghi remoti, ma tutto ciò crea anche uno scenario molto complesso, a prima vista, difficile da proteggere e da gestire



Altri fattori, non secondari, da considerare sono la mancanza di consapevolezza del rischio e di attenzione da parte del *board* direttivo, nonché la scarsità di personale OT e IT con esperienza in *cybersecurity*. Come evidenziato nell'ultima ricerca effettuata dall'*European Cyber Security Organization* (2021) sulle priorità e sfide dei responsabili della sicurezza informatica (CISO, *Chief Information Security Officers*), molti dei responsabili del settore delle *utility* considerano la *cybersecurity* non cruciale per la loro azienda o ammettono una forte difficoltà a ricevere budget dal consiglio di amministrazione che vede nella *cybersecurity* solo un costo senza ritorno sugli investimenti e non una risorsa strategica per la continuità e lo sviluppo del business.

Uno scenario quindi che sembra scoraggiare il processo di digitalizzazione delle *utility*; in realtà, rinunciare ai vantaggi delle nuove tecnologie o ignorarne i rischi non è la giusta chiave di lettura: la “quarta rivoluzione industriale” è già in atto ed è un percorso inevitabile per rimanere competitivi.

La *cybersicurezza*, come la qualità, si costruisce passo dopo passo, sulla base dell'analisi dei rischi, dell'esperienza, del feedback e della valutazione. Una protezione efficace contro gli attacchi informatici deve diventare una parte significativa dell'eredità di qualsiasi *utility*, organizzazione industriale o commerciale, insieme al rispetto delle norme ambientali, per esempio.

Del resto, il concetto di analisi del rischio, basato su criticità, probabilità e impatto, non è un concetto nuovo nel mondo della produzione e dell'industria in generale. Infatti, questa pratica è utilizzata per affrontare i rischi relativi alle infrastrutture di produzione, distribuzione e stoccaggio alla capacità di produzione (tempi di inattività della produzione), all'impatto sulle persone (lesioni, morte) e sull'ambiente (inquinamento). Questa tecnica deve semplicemente estendersi alla *cybersecurity* per affrontare i rischi inerenti ai sistemi informativi industriali.

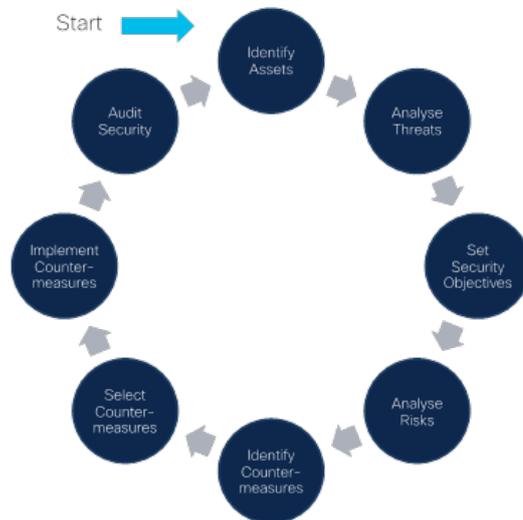
3.3.3 Cybersecurity lifecycle

Per digitalizzare i processi e i sistemi in sicurezza, le *utility* devono intraprendere una *Secure Digital Transformation* con un approccio pervasivo alla sicurezza, alla resilienza e alla *privacy* all'interno di un percorso, che per essere efficace deve ripetersi ricorsivamente.

All'interno della politica generale di sicurezza aziendale si deve definire un *Cybersecurity Management System* (CSMS), basato sull'analisi completa e coerente di tutti i rischi per l'azienda, implicando la sensibilizzazione dei *leader* aziendali, la responsabilizzazione a tutti i livelli con istruzioni che siano il

più possibile operative e coinvolgendo ogni aspetto, componente ed elemento presente in azienda, o meglio nell'intera *supply chain* aziendale: persone, policy, processi e tecnologie.

FIGURA 4 | **CYBERSECURITY MANAGEMENT SYSTEM**



Il CSMS deve fondarsi su:

- Il concetto consolidato di “difesa in profondità”, un approccio che prevede controlli di sicurezza a più livelli implementati con tecnologie e logiche diverse e complementari;
- il “principio del minimo privilegio”, dando agli utenti e ai sistemi solo i diritti e le autorizzazioni necessarie per svolgere il loro lavoro, restringendo al massimo l'accesso indesiderato ad altri dati o programmi;
- sull'assioma “Zero Trust”, la fiducia negli utenti e nei sistemi non è né binaria né permanente, occorre mettere in discussione i presupposti di fiducia ad ogni tentativo di accesso a una risorsa o a un'entità in rete, controllando i profili e le credenziali ripetutamente in equilibrio con una corretta *user experience*.

Ogni programma di sicurezza deve cominciare con l'individuazione e analisi degli *asset* da proteggere e alla loro prioritizzazione in termini di criticità e strategicità, passando, poi, all'individuazione delle possibili minacce e dei vettori di attacco interni ed esterni verso i singoli *asset*; si devono quindi decidere gli obiettivi da raggiungere per proteggere ognuno di essi, analizzando i rischi, derivanti da minacce e vulnerabilità e studiando e decidendo i controlli di sicurezza (fisici, logici e di processo) e le contromisure per bloccarli, individuarle e mitigarle. Questi controlli, in base ai paradigmi già indicati, vanno implementati in serie creando protezioni multi strato e nella fase finale del ciclo devono essere effettuati una serie di *assessment* o *auditing* delle soluzioni utilizzate, eseguendo test sulla qualità e affidabilità dei controlli prima di ricominciare un nuovo ciclo volto a migliorare quanto già realizzato.

In questo processo iterativo, i team dell'*IT Security Operation* (SecOps) e dell'*OT Engineering* devono essere coinvolti con posizioni e responsabilità paritarie e complementari, in quanto i domini IT e OT presentano peculiarità e differenze sostanziali. L'*IT security* punta alla protezione dei dati e dei sistemi di informazione dagli accessi non autorizzati, implementando procedure, policy e controlli che garantiscono confidenzialità, integrità e disponibilità delle applicazioni e dei sistemi di trasmissione elaborazione e storage dei dati, mentre nel dominio OT, occorre far riferimento anche alla sicurezza

fisica (*safety*), ovvero proteggere l'integrità di persone, apparati e i siti produttivi, focalizzandosi maggiormente sulla continuità operativa e sulla corretta funzionalità degli impianti. Di conseguenza, contromisure, controlli e metodi di protezione da adottare sono sostanzialmente differenti nei 2 domini e nel contesto di transizione 4.0 (ad esempio industria 4.0) vanno visti come complementari, integrati e, alla luce dei recenti attacchi, estesi all'intera *supply chain* aziendale.

3.3.4 Supply Chain Security

In base al rapporto pubblicato dall' *Agenzia dell'Unione europea per la cybersicurezza*, (ENISA, European Network and Information Security Agency) a luglio 2021³, il numero di attacchi informatici alla catena di approvvigionamento (*supply chain*) delle aziende quadruplicherà nel corso del 2021 rispetto al 2020 e, come evidenziato dal sofisticatissimo attacco alla piattaforma *software Solarwind Orion*⁴ (dicembre 2020), la metà di questi attacchi proverrà da cybercriminali sponsorizzati da Stati sovrani (cosiddetti *Advanced Persistence Threat (APT) actor*), dotati di mezzi e tecnologie tali da poter orchestrare attacchi molto complessi e duraturi verso obiettivi mirati.

Le utility, in qualità di fornitori di servizi essenziali per il paese, devono prepararsi a tale evenienza in maniera duplice, e devono:

- Estendere i programmi di sicurezza ai loro fornitori e ai partner
- Implementare controlli di sicurezza all'interno dell'intero ciclo di vita dei prodotti e servizi che forniscono, dalla loro ideazione sino alla loro dismissione finale.

La globalizzazione e ramificazione delle aziende, la loro interdipendenza nonché l'acquisizione e stoccaggio di tecnologia e materiali in maniera decentralizzata, e la complessità della catena logistica, sono fattori che le espongono a minacce interne ed esterne di varia natura, quali spionaggio, manipolazione o uso improprio di informazioni riservate o di credenziali di accesso, contraffazione dei sistemi e apparati utilizzati, diffusione di informazioni personali che possono concretizzarsi in attacchi in vari punti e momenti della filiera e rete produttiva.

Il rischio o le minacce sono spesso dovuti alle differenze di obiettivi, aspettative, scadenze, *budget* e priorità di sicurezza delle persone o aziende coinvolte a diverso titolo nella catena.

Non è sufficiente avere aziende partner e fornitori con una loro *policy* di sicurezza, occorre creare con loro una relazione di genuina fiducia. Il concetto di *Trust* deve essere alla base dei processi di digitalizzazione delle *utility* e questo significa anche affidabilità, responsabilità nelle infrastrutture e nelle soluzioni alla base della loro trasformazione digitale; collaborazione e trasparenza con i soggetti pubblici e privati e con le persone che operano i servizi all'interno della *supply chain* e con gli utenti. La sicurezza pervasiva può essere raggiunta solo se ci si coordina in modo significativo con i colleghi della catena del valore, solo comprendendo i modelli di business dei partner si può abilitare la sicurezza.

Occorre, quindi, attraverso un continuo allineamento e vari strumenti:

- Stabilire l'insieme comune di minacce alla sicurezza
- Riunirsi intorno a obiettivi chiari che possono essere raggiunti solo collettivamente
- Comprendere gli aspetti commerciali unici di ogni partner nella catena
- Rivelare apertamente le sfide e le difficoltà

³ Threat Landscape for Supply Chain Attacks

⁴ <https://spycloud.com/solarwinds-attack-breakdown/>

- Condividere strategie tecniche di sicurezza, pratiche operative e successi

In altre parole, la sicurezza delle informazioni deve essere un lavoro primario e prioritario di tutti gli attori coinvolti.

Anche in questo caso occorre seguire un approccio strutturato mediante l'implementazione di un *Supply Chain Risk Management Systems* che, facendo riferimento a *framework standard* (ad esempio ISO 28000:2007) e tecnologie consolidate, estenda i programmi a tutti gli anelli e partner dell'ecosistema aziendale.

La sicurezza comincia con la consapevolezza del rischio, quindi il fattore umano, che rappresenta il vero anello debole della catena, deve essere il primo obiettivo di tutti i programmi di sicurezza: occorre lavorare sull'aspetto culturale e comportamentale di tutto il personale e attori coinvolti nei processi aziendali.

Un'altra nota specifica meritano gli apparati, le applicazioni e i sistemi IT/OT in generale, essendo il vero obiettivo degli attacchi ma anche il mezzo principale attraverso il quale va implementata la sicurezza. La sicurezza in profondità parte dal basso, dall'ideazione, progettazione e sviluppo o acquisizione dei sistemi, che devono essere:

- costruiti su piattaforme di tecnologie affidabili, in grado di garantire componenti *hardware* e *software* integri, la cui integrità va mantenuta e verificata nel tempo, attraverso la costante raccolta di dati;
- sviluppati secondo processi documentati, misurabili, ripetibili e che prevedano un approccio *security & privacy by design*;
- ridondanti, con capacità a livello *hardware* e *software* di aumentare la propria resilienza e integrità;
- aderenti ai principali standard internazionali di *best practice* e *Information Assurance*.
- inventariati, tracciati e controllati mediante un processo di *procurement* che certifichi i fornitori e i canali di acquisizione, trasporto e stoccaggio.

3.3.5 Sicurezza e Resilienza delle *Critical Entities* nelle Direttive Europee

La protezione dalla crescente minaccia cibernetica per le infrastrutture critiche e gli operatori di servizi essenziali (OSE), fornitori di energia, acqua e gas in primis, è da qualche anno una priorità nelle agende dei legislatori europei e italiani.

Si riportano, pertanto, qui di seguito stralci delle principali direttive e normative emesse dalla Commissione e dal Parlamento dell'Unione Europea in tema di *cybersecurity* e *privacy*, nonché cenni ai decreti della Presidenza del Consiglio dei Ministri e alle leggi che, recependo tali direttive, hanno definito il *Piano nazionale per la protezione cibernetica e la sicurezza informatica* istituendo L'Agenzia per la *Cybersicurezza Nazionale* (ACN) e il *Perimetro Nazionale di Sicurezza Cibernetica* (PNSC).

3.3.5.1 Direttive dell'Unione Europea, *Network and Information Security (NIS)*

La direttiva UE del Parlamento europeo 2016/1148, nota come NIS, *Network and Information Security*, è il primo pezzo di legislazione in ambito *cybersecurity* nell'Unione Europea. In quanto direttiva e non regolamento, ha costretto gli Stati membri ad adottare una legislazione nazionale in materia, ma ha lasciato loro una certa flessibilità nell'interpretazione e trasposizione, che andavano, comunque, ultimate a maggio 2018.

La direttiva obbliga ogni paese UE a sviluppare una strategia nazionale e una determinata capacità nazionale di *cybersecurity*, (CSIRT nazionale, esercitazioni cibernetiche, obblighi la notifica di incidenti, ecc.), a collaborare con gli altri paesi dell'UE scambiando informazioni e allarmi, tramite la rete operativa dei CSIRT EU, il gruppo di cooperazione strategica NIS e l'*Agenzia dell'Unione Europea per la Cybersecurity* (ENISA), e a effettuare la supervisione della cybersicurezza degli operatori essenziali (energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile) e dei fornitori di servizi digitali e finanziari critici (motori di ricerca, servizi cloud e portali di e-commerce).

In particolare, viene rilanciato il ruolo dell'ENISA, che deve identificare:

- *best practice* nell'attuazione della direttiva NIS stessa;
- sostenere il processo di segnalazione degli incidenti di cybersicurezza in tutta l'UE;
- sviluppare soglie, modelli e strumenti;
- concordare approcci e procedure comuni;
- aiutare gli Stati membri ad affrontare questioni comuni di sicurezza informatica.

La direttiva NIS è stata recepita in Italia tramite il decreto legislativo n.65 del 18/05/2018. Solo successivamente, tramite altri decreti attuativi, come spiegato nei paragrafi successivi, sono stati istituiti il *Perimetro Nazionale di Sicurezza Cibernetica*, e nel giugno 2021 la maggior parte delle responsabilità e autorità competenti NIS sono state consolidate nell'*Agenzia per la Cybersicurezza Nazionale*, mentre inizialmente erano distribuite, per motivi di competenza, su ben 5 ministeri.

3.3.5.2 La Nuova Strategia Digitale Europea e Proposta NIS 2

Nel dicembre 2020, la Commissione Europea ha presentato la nuova strategia digitale volta a proteggere Internet, i dati personali ma anche i valori e diritti fondamentali di ogni cittadino europeo, e ha lanciato 2 proposte di direttive relative a “misure per un alto livello comune di cybersecurity” (anche detta “NIS 2”) e alla resilienza delle entità e reti critiche.

Le proposte coprono un ampio numero di settori e mirano a indirizzare i rischi attuali e futuri relativi ad attacchi informatici, criminali e ai disastri naturali in maniera complementare.

La nuova strategia contiene proposte di regolamenti, investimenti e *policy* in 3 aree:

- Resilienza, sovranità e *leadership* tecnologica
- Capacità operativa di prevenzione, deterrenza e risposta
- Cyberspazio globale e aperto tramite la collaborazione

La proposta di direttiva NIS 2, alla luce dei limitati e frammentati risultati raggiunti dalla NIS 1, vuole riformare le regole per sicurezza delle reti e dei sistemi informatici pubblici e privati, per aumentare il livello di resilienza delle infrastrutture critiche.

In particolare, per superare i problemi legati alla non chiara definizione di “operatori di servizi essenziali” e fornitori di servizi digitali, propone di estendere l’ambito applicativo della NIS 1, categorizzando le infrastrutture critiche in:

- Entità essenziali, ovvero energia, spazio, trasporti, banche, mercato finanziario, acqua potabile e acque reflue, delle infrastrutture digitali, della salute, della pubblica amministrazione;
- Entità importanti, cioè industria alimentare, servizi postali, gestione dei rifiuti, industria chimica, fornitori digitali.

La direttiva precisa anche che l'ambito di applicazione della supervisione da parte dell'ente di Stato demandato deve essere legato alle dimensioni dell'entità, l'importanza e l'impatto dei possibili incidenti, tenendo di fatto fuori le piccole e medie imprese.

La proposta inoltre mira a disciplinare gli obblighi dei vari paesi EU in termini di misure tecniche e organizzative, introducendo il concetto di proporzionalità in relazione ai possibili rischi, minacce e impatto nonché di notifica degli incidenti e condivisione di informazioni, allarmi e minacce.

3.3.6 Agenzia per la Cybersicurezza Nazionale

Oltre le Autorità di riferimento per il settore delle *utility* (ARERA, AGCM, Garante Privacy, ANAC, ecc.) recentemente - il 3 agosto 2021 - il Parlamento ha approvato in via definitiva il disegno di legge di conversione del decreto legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'*Agenzia per la cybersicurezza* (ACN), accelerando notevolmente, alla luce del PNRR, lo sviluppo e l'attuazione dell'architettura nazionale di cybersecurity, considerata fondamento della trasformazione digitale del paese.

All'Agenzia - che ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria - spetta in particolare:

- predisporre la strategia nazionale di cybersicurezza;
- assumere compiti finora attribuiti a diversi soggetti, quali il ministero dello Sviluppo Economico, la Presidenza del Consiglio, il Dipartimento delle informazioni e della sicurezza, l'Agenzia per l'Italia digitale;
- promuovere iniziative per lo sviluppo di competenze e capacità.

04

LA DIGITAL UTILITY



4 La Digital Utility

4.1 Un nuovo perimetro di business per la “Digital Utility”

Dopo un lungo periodo pre-liberalizzazione dei vari mercati, caratterizzato da sostanziale stabilità e staticità di contesto, le *utility* da diversi anni a questa parte stanno affrontando una nuova era di evoluzione e cambiamento.

La rivoluzione digitale si è presentata prepotentemente nel settore dell'energia e dei servizi ambientali. Le energie rinnovabili, la generazione distribuita e le reti intelligenti richiedono nuove competenze e stanno attivando nuovi modelli di business e l'adeguamento dei quadri normativi e legislativi. La raccolta e lo scambio di dati come riportato nel capitolo 1 mostrano una crescita esponenziale, creando inevitabili minacce digitali ma anche preziose opportunità. La competizione per contendersi i clienti si sta spostando sul canale online; l'Internet delle cose (IoT) promette nuovi prodotti e opzioni di gestione. I protagonisti mondiali dell'economia digitale stanno sconvolgendo il panorama industriale, mentre i governi e gli organismi di regolamentazione cercano di incoraggiare sistemi di misurazione più intelligenti e standard più ecologici per la generazione e il consumo.

Per creare valore per gli *stakeholders* e gli *shareholders* in mezzo a queste sfide, la *Digital Utility* del futuro si troverà a dover operare in un sistema prevalentemente digitale. Ciò significa che le *utility* dovranno perseguire una strategia di adattamento costante in ottica di trasformazione digitale della propria organizzazione e delle attività. L'anticipare queste mosse per migliorare l'efficienza ed espandere la base di clienti è un fattore critico di successo. Man mano che la trasformazione conquisterà una sempre più ampia base di clienti anche per una loro naturale inclinazione generazionale alle nuove tecnologie, questo slancio aprirà opportunità digitali più profonde in un ampio campo. Le opportunità sono presenti lungo tutta la catena del valore dell'industria energetica, dalla generazione di energia, all'organizzazione dei servizi alla gestione delle relazioni con i clienti finali. Poiché le *utility* sono legate storicamente al loro territorio e perseguono queste opportunità, sarà sempre più concreta l'interazione con i clienti finali, specie in condizioni di stress dei prezzi dell'energia. Molte *utility* hanno lanciato applicazioni mobili per la notifica, la presentazione e il pagamento delle fatture, nonché per la gestione dei disservizi. In poco tempo, le applicazioni mobili si estenderanno in modo sempre più pervasivo alle “case intelligenti”, agli edifici connessi, alla mobilità elettrica. La gestione digitale delle risorse energetiche distribuite, dai singoli siti a interi sistemi, è già realtà. Molti progetti all'interno dell'*utility* hanno un focus digitale e utilizzano tecniche dell'economia digitale, come lo sviluppo tramite integrazione di *startup*. Sono evidenti le prospettive dell'innovazione di breve-medio periodo, attraverso l'analisi di fenomeni altamente rilevanti come gli investimenti di *Corporate Venture Capital*, condotti da *utility*, fornitori di tecnologia e imprese automotive, o come le recenti acquisizioni di *startup* innovative appartenenti all'ecosistema dell'energia, considerando anche le *startup* più giovani e ancora indipendenti che potranno fare la differenza negli anni a venire.

La trasversalità di questi fenomeni sta abbattendo le barriere tra mercati: l'energia non è più semplicemente un'industria, chiaramente distinguibile da altri settori, quanto un ecosistema di imprese interconnesse e interdipendenti (come nel caso della mobilità elettrica). Tali fenomeni sono accelerati dai rapidi cambiamenti tecnologici che abbattano le barriere all'ingresso e abilitano nuovi modelli di business ICT e strumenti di *cybersecurity* e *data analytics*. Si evidenzia che tali investimenti vengono effettuati sia in ottica *driving*, al fine di migliorare l'offerta già esistente delle *utility* (ad esempio: protezione della rete intelligente da cyber attacchi), sia in ottica *emergent* al fine di monitorare tecnologie attualmente *no core*, ma che potrebbero creare *disruption* nel mercato nel futuro. Ciò

rinforza l'idea che le *utility* stiano affrontando una trasformazione verso lo status di "fornitori di servizi", abilitati dalle tecnologie digitali.

4.2 Le sfide della *Digital Utility*

Non di rado, i potenziali benefici di una pianificazione strategica della digitalizzazione vengono sottovalutati. L'esperienza storica in altri settori ha già rivelato che i possibili ritorni degli investimenti nella digitalizzazione sono maggiori di quanto credessero i promotori dei progetti stessi. La società di logistica statunitense *United Parcel Service*, ad esempio, negli anni '90 aveva introdotto il *track and trace* per i pacchi, con l'obiettivo di migliorare l'offerta per i clienti (sistema oggi assolutamente imprescindibile nelle dinamiche dell'*e-commerce*). Solo in seguito è diventato chiaro che l'uso dei *Dati* grazie alla digitalizzazione ha consentito una migliore gestione di pacchi, veicoli e processi di distribuzione. Alla fine, l'azienda ha migliorato l'efficienza nell'intero ambito delle sue operazioni e ha risparmiato centinaia di milioni di dollari.

In questo ambito si sta consolidando l'approccio di affiancare ai tradizionali sistemi di supervisione di processo (ad esempio i sistemi SCADA) la raccolta di dati complementari provenienti dagli *asset* strategici distribuiti: il fine è quello di monitorare e gestire in tempo reale gli impianti, rilevare con maggiore granularità i consumi dei clienti, quantificare i flussi energetici, fare un inventario continuo e in tempo reale dei propri *asset* distribuiti, aumentare le interazioni con i clienti, rendere più efficienti i processi operativi e incrementare il livello di sicurezza dei propri dipendenti.

L'avvento di nuove tipologie di connettività wireless IoT di nuova generazione, come il 5G, di tipologia *Low Power Wide Area Range* (ad esempio LORAWAN) e *Narrow Band IoT*, è sicuramente un abilitatore per questi nuovi scenari.

La crescente mole di dati che ne deriva costituisce per le *utility* una grande opportunità di evoluzione e al contempo una sfida aziendale volta a trasformare tali dati in reale valore. Perché questo accada è però condizione necessaria che il processo di digitalizzazione debba essere intrapreso in modo sistemico e integrato, sia all'interno dell'organizzazione dell'operatore che in tutti i processi aziendali che governano il ciclo di vita dell'energia, con l'obiettivo finale di costituire una vera e propria *Data Driven Utility*.

Come descritto nei precedenti paragrafi, il dato grezzo, che si deve caratterizzare il più possibile per la qualità oltre che per la quantità, si trasforma progressivamente in informazione, conoscenza, consapevolezza e supporto effettivo alle decisioni e azioni da intraprendere. Sulla base dell'esperienza di altri settori, le *utility* possono dare seguito a obiettivi digitali ambiziosi. Possono pianificare con sicurezza miglioramenti trasformativi in termini di produttività, affidabilità, sicurezza, esperienza del cliente, efficienza nella gestione caratteristica del servizio. Le dimensioni di queste interessanti opportunità possono essere comprese in 3 fasi di sviluppo legate a:

- Produttività ed efficienza
- Esperienza del cliente
- Nuove frontiere per il proprio business

4.3 Il cliente al centro

Le *utility* nel settore della vendita al dettaglio, come negli ambienti regolamentati tradizionali, stanno lottando per fidelizzare i clienti e far fronte alla pressione competitiva delle nuove forme di generazione distribuita (ad esempio l'autoproduzione, comunità energetiche ecc.). Digitalizzando l'esperienza del cliente, le *utility* possono contemporaneamente migliorare la soddisfazione commerciale e ridurre i costi. In alcuni segmenti *cross* c'è anche il potenziale per aumentare il fatturato. A sostegno dell'opportunità, negli ultimi anni quasi tutti i principali fornitori di energia hanno investito in canali online e non ultimo nel *mobile*. Mentre molti degli sforzi hanno prodotto risultati interessanti, alcuni restano indietro rispetto all'usabilità e all'interfaccia tra i canali di vendita online e tradizionali.

La maggior parte dei clienti apprezza una piattaforma multicanale che collega perfettamente le loro interazioni su tutti i canali: *online*, *mobile*, *call center* e vendita diretta. Per i servizi pubblici, i processi che vedono il coinvolgimento attivo del cliente mostrano livelli qualitativi incrementali. Inoltre, l'adozione di piattaforme multicanale sempre attive (*always on*) è un requisito per una proficua e interessante analisi del comportamento dei clienti durante l'intero "percorso di consumo". Le *utility* che utilizzano analisi avanzate per migliorare la qualità del servizio, ridurre i costi e approfondire le relazioni con i clienti, attraverso l'analisi dei *Dati* dei clienti sono quelle che riscontrano miglioramenti significativi nella gestione interna dei processi, inclusa l'analisi e la gestione degli errori.

4.4 Visione digitale e posizionamento

In coerenza con tutte le precedenti versioni dell'*Orange Book*, in quest'ultimo paragrafo si vuole offrire un percorso di lettura della digitalizzazione nell'ottica del suo contributo al cambiamento dei confini e delle dinamiche del settore.

Nell'articolare la propria visione digitale, le aziende dovrebbero per prima cosa identificare la posizione che vogliono occupare nell'ecosistema digitale, rispetto a dati, servizi e dispositivi.

Più precisamente, questo significa trovare i punti della catena del valore in cui la digitalizzazione darebbe il maggior contributo al business, ad esempio nell'arco temporale di riferimento, come un triennio.

Le aree di azione per le trasformazioni digitali sono descritte nella figura 7.

Attraverso un'analisi sistematica, le aziende possono apprendere l'opportunità di valore di ciascuna area e la fattibilità del raggiungimento degli obiettivi.

Elevare l'importanza del *design*. Come dimostrano i prodotti e i servizi delle *big tech* statunitensi, la semplicità del *design* e soprattutto prodotti finali di facile utilizzo sono fattori ad alto valore aggiunto nell'economia digitale. Le trasformazioni digitali di successo dipendono chiaramente dalle dinamiche con cui vengono adottate e utilizzate. Alla strategia e alla tecnologia, i due principali ingranaggi di lavoro delle tradizionali trasformazioni aziendali, deve quindi essere aggiunto il *design* come terzo prerequisito dello sforzo e investimento nella digitalizzazione. L'analisi *post mortem* dell'esperienza dell'utente non è il percorso migliore verso un processo di successo. Gli utenti finali, siano essi clienti, fornitori o dipendenti, devono contribuire a plasmare il progetto sin dall'inizio e fornire *input* costanti sull'usabilità e l'utilità di qualsiasi sforzo digitale. cambiamento comportamentale o professionale proposto.

FIGURA 4 | AREE DI AZIONE PER LE TRASFORMAZIONI DIGITALI

Nuove Frontiere		
Temi di business	<ul style="list-style-type: none"> • Smart grid & meters • Smart homes • Connected buildings • Generazione distribuita 	<ul style="list-style-type: none"> • Servizi ambientali ed energetici • Manutenzione predittiva • Mobilità sostenibile (elettrica ecc.) • Digital commerce
Fulcro della trasformazione		
Cura del design in ottica cliente (interno/esterno)	<ul style="list-style-type: none"> • Processi digitali front-end • Multichannel commerce • Digital marketing and social media 	<ul style="list-style-type: none"> • Esperienza digitale e fisica integrate • Customer life-cycle management • Customer experience management
Prodotti e servizi digitalizzati	<ul style="list-style-type: none"> • Open innovation • Digital innovation 	<ul style="list-style-type: none"> • Intelligent products and components
Catena del valore	<ul style="list-style-type: none"> • Processi automatizzati di back-end • analytics e intelligenza artificiale 	<ul style="list-style-type: none"> • End-to-end digitization • Supporto alla produttività dei dipendenti
Principi tecnici e organizzativi		
Tecnologia	<ul style="list-style-type: none"> • Architettura dei Sistemi e dei dati • Smartphone • Connettività 	<ul style="list-style-type: none"> • Big data/smart data and advanced analytics • Data security
Cultura e organizzazione	<ul style="list-style-type: none"> • Project culture • Collaborazione cross-funzionale • Orizzontalità gerarchica 	<ul style="list-style-type: none"> • Meritocrazia e supporto ai talenti digitali • Leggerezza organizzativa

Fonte: elaborazione ADL Consulting

L'approccio agile. L'approccio a una progettazione di successo è strettamente legato al passaggio a una filosofia di gestione e sviluppo agile e iterativa dell'organizzazione. L'approccio agile al cambiamento si basa su una cultura della condivisione, su una comunicazione aperta e su un supporto e una presenza visibili da parte del top management. Utilizzando *team* interfunzionali è possibile migliorare la progettazione per comprendere più a fondo gli utenti finali e soddisfare le loro esigenze in modo più accurato. A differenza di un approccio ingegneristico convenzionale, i *team* lavorano secondo un principio iterativo di test e apprendimento. Il *top management* farebbe bene a concedere a questi *team* la massima libertà possibile quando si tratta di agire (sui principi di delega e controllo), poiché l'esperienza dimostra che i team agili favoriscono il successo nel processo di trasformazione digitale.

Partire dall'utente/cliente finale. Un approccio aziendale orientato all'utente finale supporta il ruolo del design e quello di una filosofia basata sull'agilità. Durante la fase di digitalizzazione dei processi aziendali, le aziende che hanno avuto maggior successo sono partite dall'utente finale e hanno lavorato a ritroso (*reverse engineering*). Questo approccio aiuta a garantire che le iniziative siano intraprese in base al loro valore sul mercato dei servizi e alla riscontrata esigenza e richiesta di cambiamento. Una volta compreso come i clienti interagiscono passaggio per passaggio, si può inquadrare il valore insito nel cambiamento di gestione e nell'ampliamento del perimetro di business che ne potrebbe conseguire.

Alla turbolenza e alla complessità si risponde con la leggerezza organizzativa che privilegia l'intelligenza, la creatività e le idee. (Ispirato a Italo Calvino, Lezioni Americane 1985)

Autori e contributi: Francesca Mazzarella, Claudio Di Mario, Marialessandra Carro, Pietro Quercia, Michele Festuccia, Giovanni Colombo.

05

APPENDICE
CASI
D'USO



5 Appendice - Casi d'uso

In questa appendice vengono affrontati alcuni casi d'uso e progetti implementati presso *power utility* che hanno intrapreso con determinazione il processo di digitalizzazione contemplato nei principi, *driver* di mercato, forme e linee guida sin qui trattate.

5.1 Sensorizzazione e IoT

La tecnologia di connettività IoT LORAWAN si è dimostrata particolarmente adeguata alla prevenzione dei furti di rame e in generale di *asset* critici posizionati in siti operativi e cantieri non presidiati. Specifici sensori dotati di localizzatore GPS, da applicare su bobine di rame, (Fig. 8) abilitano servizi di *geo-fencing* e ricostruzione storica dei percorsi, e quindi consentono di rilevare in tempo reale movimentazioni sospette oltre limiti e confini predefiniti.



Illustrazione ADL Consulting

La tecnologia LORAWAN è in grado di fornire nativamente il servizio di geo-localizzazione, introducendo algoritmi di triangolazione TDOA/RSSI: una volta messi in atto opportune accortezze sul *capacity planning* della rete, in questo modo si conseguono i vantaggi di ridurre ulteriormente il costo dei sensori e il consumo degli stessi.

In ambito *multiutility* una serie di applicazioni di *smart city* possono essere abilitate mediante la tecnologia LORAWAN e sensoristica specializzata, come ad esempio *smart parking*, monitoraggio della qualità dell'aria e delle condizioni meteorologiche, gestione ottimizzata della raccolta dei rifiuti, gestione dell'illuminazione pubblica.



Illustrazione ADL Consulting



Illustrazione ADL Consulting

5.2 Software Defined Network e Utility Digital Network

Riveste particolare interesse il *trend* che diverse *utility* elettriche stanno recentemente consolidando sul fronte dell'adozione di connettività in fibra ottica delle proprie sottostazioni elettriche di distribuzione primarie e secondarie, in sinergia a logiche di rete *software defined*. Vengono in tal modo conseguiti i seguenti vantaggi:

- Lo scambio dati “orizzontale” tra le sottostazioni appartenenti alle stesse linee di media tensione si caratterizza per una maggiore affidabilità e una riduzione consistente delle latenze. In tal modo gli algoritmi di automazione distribuita diventano più efficienti restituendo una rete elettrica molto più affidabile in grado di aumentare la qualità del servizio elettrico offerto e ridurre le penali emesse dall’authority per le interruzioni di servizio.
- L’aumento del *throughput* in rete consente non solo di aumentare le capacità di supervisione di processo ma anche di installare una sensoristica diffusa nelle sottostazioni e sulle linee elettriche, al fine di aumentare la capacità di monitoraggio del sistema elettrico e adottare modelli di manutenzione predittiva.
- Semplificazione architetturale in quanto protocolli, tipicamente di livello 2 ISO/OSI, come l’IEC 61850 GOOSE, possono essere più agilmente trasmessi senza ricorrere a complicate tecniche di *overlay* di rete.
- Minori costi operativi e rilascio più agile e veloce di nuovi servizi e applicazioni, grazie alla presenza di un controllore di rete in grado di attuare logiche di *plug-and-play* per la prima attivazione, riconfigurazione *software-defined* delle funzionalità di rete e delle tecniche di separazione e segmentazione del traffico.
- Maggior sicurezza in quanto, grazie a tecniche di automazione, si riducono drasticamente le possibilità di errori umani di configurazione; è possibile altresì attuare tecniche di cifratura ad alte prestazioni sul traffico delle sottostazioni anche di livello 2.
- Gli apparati di rete *rugged*, industriali e *compliant* allo standard IEC61850-3, se dotati di capacità di *edge computing*, possono favorire la virtualizzazione e il consolidamento su un unico *hardware*, affidabile e validato, di diverse applicazioni residenti in sottostazione riscritte con formati software leggeri come *Linux container* e *Docker*. In tal modo si riducono sensibilmente i CAPEX e gli OPEX, gli spazi, i “sistemi di raffreddamento” e i consumi ad essi legati che spesso diventano critici nelle numerose infrastrutture distribuite sul campo e non presidiate.

5.3 Sostenibilità e resilienza delle città

Nel corso degli ultimi anni, il Comune di Milano ha aderito ad alcuni impegni internazionali (*Patto dei Sindaci*, *Carta di Bologna per l'Ambiente*, *Deadline 2020 di C40*) che si traducono in strumenti di pianificazione e azioni a livello locale, per dare seguito alla mozione relativa alla *Dichiarazione di emergenza climatica e ambientale* approvata dal Consiglio comunale.

Safer Milan è un progetto di co-innovazione, citato nelle *Linee guida per l'adattamento ai cambiamenti climatici* della città di Milano, focalizzato su: monitoraggio ambientale e idrogeologico, emergenze, sicurezza fisica e *cybersecurity*.

Le attività progettuali hanno preso il via nel corso del 2018 con l'obiettivo di toccare diversi ambiti:

- Integrazione e rafforzamento dei sistemi di sicurezza fisica, di monitoraggio idrogeologico, di monitoraggio ambientale già in essere, con reti e piattaforme adeguatamente protette utilizzando le più evolute soluzioni di *cybersecurity*;
- La creazione di un centro di innovazione dedicato allo sviluppo di soluzioni innovative per la sicurezza - in particolare nell'ambito cittadino - in cui *startup*, università e aziende possano collaborare, contribuendo a fare della città di Milano un esempio di eccellenza internazionale e di attrazione nel settore;
- L'ampliamento dell'offerta di formazione in ambito *cybersecurity* e IoT, attraverso i corsi specialistici⁵.

In particolare, intorno al tema della resilienza ai fenomeni estremi generati dai cambiamenti climatici, il progetto *Safer Milano* ha permesso di sviluppare, in collaborazione con la Protezione Civile e con la Polizia Locale della Città Metropolitana, due diversi sistemi di monitoraggio e controllo:

- Un sistema di monitoraggio del corso dei 3 fiumi che toccano l'area metropolitana (Olona, Seveso e Lambro) per rilevarne costantemente il livello e per conoscere, attraverso una rete di pluviometri, la quantità di precipitazioni che incidono nelle diverse zone.
- Una soluzione di monitoraggio dei sottopassi stradali che, a causa dell'intensità degli eventi atmosferici, soffrono sempre più spesso di improvvisi allagamenti, motivo di forte preoccupazione sia per l'amministrazione pubblica sia per la cittadinanza.

Nel primo caso, serviva una soluzione che desse immediatezza e facile interpretazione dei dati rilevati dai sensori in campo. Grazie alla nuova piattaforma, è possibile visualizzare graficamente sia indicazioni puntuali sia sviluppo di *trend* relativi al livello idrometrico dei 3 alvei fluviali in diversi punti del loro corso (Fig. 10)

⁵ Cisco Networking Academy

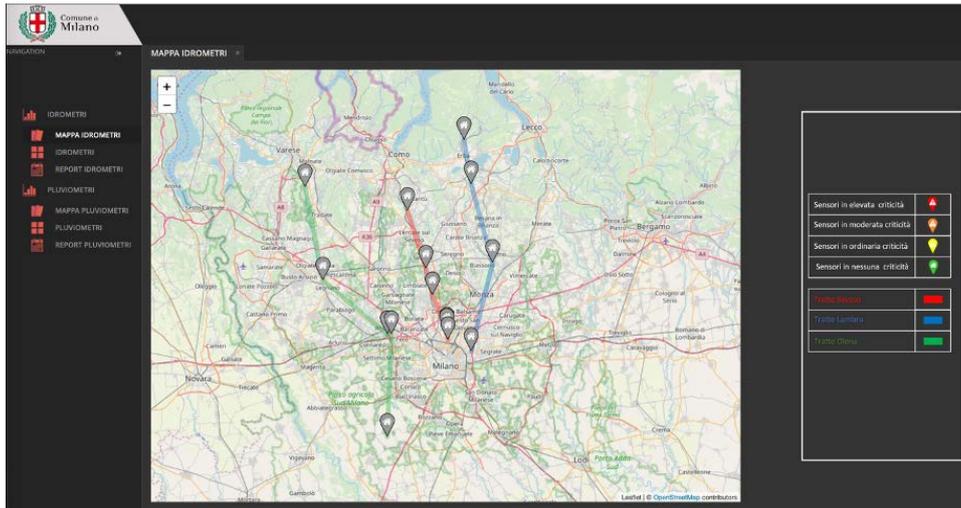


Illustrazione ADL Consulting

Allo stesso tempo, una serie di sensori distribuiti in tutta l'area metropolitana, fornisce dati sulla quantità di precipitazioni in atto con lo scopo di stimare l'impatto che potrebbero generare (Fig. 11). La piattaforma aiuta la Protezione Civile a mettere in atto in modo tempestivo attività di prevenzione e notifica alla cittadinanza. A tali informazioni potranno aggiungersi elementi accessori quali, ad esempio, flussi video provenienti da telecamere installate lungo il corso dei fiumi, previsioni meteorologiche.



Illustrazione ADL Consulting

L'obiettivo del secondo ambito progettuale è quello di fornire alla Protezione Civile e alla Polizia Locale della Città Metropolitana di Milano uno strumento di monitoraggio dei sottopassi che possa dare riscontri in tempo reale circa i possibili allagamenti provocati da fenomeni temporaleschi. Inoltre, laddove richiesto, la piattaforma consente di intervenire con strumenti di controllo del traffico veicolare (pannelli a messaggio variabile e/o semafori) per bloccare il transito dei mezzi nelle situazioni di pericolo.

Attraverso sensori di livello, montati sulla travatura superiore del sottopasso e sensori di presenza di acqua montati a livello del suolo, è possibile rilevare gli eventuali allagamenti e la loro gravità. La

presenza di una telecamera permette di controllare lo stato del sottopasso ed eventuali situazioni di pericolo che richiedano un intervento immediato.

Grazie a pannelli a messaggio variabile, posizionati opportunamente sulle vie di ingresso al sottopasso, è possibile reindirizzare il traffico su altri percorsi in caso di impraticabilità della strada.

Queste informazioni giungono in tempo reale sia alla Protezione Civile sia alla Polizia Locale per consentire loro di definire strategia e tipologia di intervento in loco fig. 12.

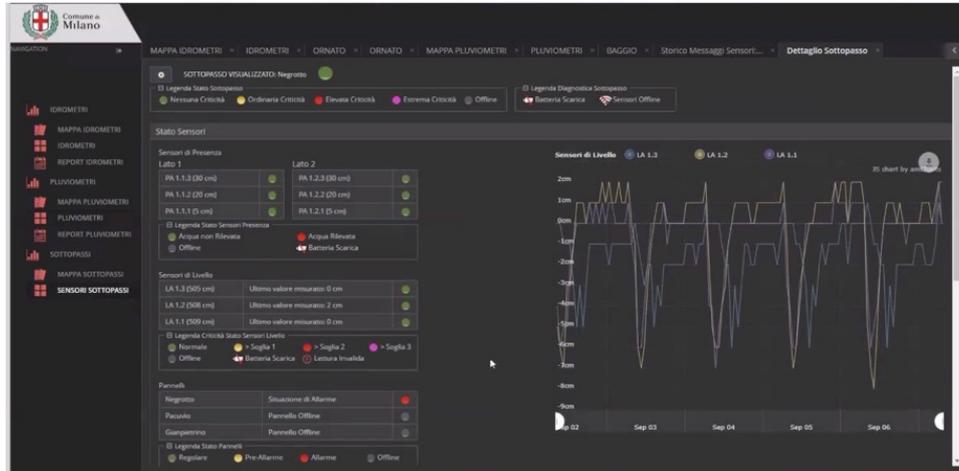


Illustrazione ADL Consulting

La collaborazione con la *multiutility* locale, oltre a velocizzare la realizzazione delle opere, ha permesso di sfruttare per gli scopi progettuali sia la rete di fornitura dell'energia sia la rete di comunicazione LORAWAN per la raccolta dei dati prodotti dai sensori IoT. Una soluzione di cybersicurezza a più livelli protegge gli accessi al sistema ed i dati raccolti.

5.4 Automazione e messa in sicurezza di un impianto per la gestione delle acque reflue

Enti e aziende che scelgono un percorso di trasformazione digitale hanno come principale obiettivo il raggiungimento di un valore (precedentemente indicato come catena del valore) tangibile e misurabile, auspicabilmente in determinati termini temporali.

Tale risultato non può prescindere da una fase preliminare della progettualità che parte dall'analisi degli obiettivi e requisiti ed una conseguente qualificazione del contesto mettendo in evidenza il divario tra l'esistente ed il desiderato (*gap analysis*).

Ciò consente una successiva e corretta identificazione degli interventi necessari e la pianificazione degli stessi nonché una valida analisi costi/benefici. È giustificata in questo modo sia la convenienza del raggiungimento degli obiettivi iniziali previsti, oltre che in molti casi, l'ottemperare primariamente a regolamentazioni e normative vigenti nel contesto valutato.

La volontà di trovare soluzioni capaci di assolvere la *compliance* delle regolamentazioni, di migliorare "l'esperienza del consumo della risorsa acqua" degli utenti finali, e di ottimizzare operatività e sicurezza degli impianti stessi, può essere tra i principali *business value* che giustificano e sostengono gli interventi progettuali in ambito trattamento acque.



Illustrazione ADL Consulting

Le relazioni che coinvolgono sistemi tecnologici, nonché cose (IoT), dati, persone e processi, risultano essere i primari elementi oggetto della trasformazione digitale. Questo paradigma è sempre più attuale per sistemi e impianti di medie e grandi aziende, e ultimamente interessa infrastrutture critiche del sistema paese in particolare in ambito di gestione e trattamento delle acque.

Sul piano tecnologico, le principali ragioni su cui si può considerare attuale e di forte interesse un percorso di trasformazione digitale dei sistemi in ambito trattamento acque, da qui *smart water system*, può ricondursi principalmente alle necessità di:

- mitigare gli ingenti effetti dovuti ad azioni malevoli in ottica *cybersecurity* nonché errori umani;
- realizzare l'efficientamento degli impianti in termini di sostenibilità e *green*;
- attuare una razionalizzazione delle operatività e relativi costi di gestione degli asset.

Confermano tale forte interesse alla digitalizzazione sia le tendenze di mercato nell'adozione di piattaforme in ottica IoT e cybersecurity, che di sistemi di controllo e automazione sia di impianti che di processo.

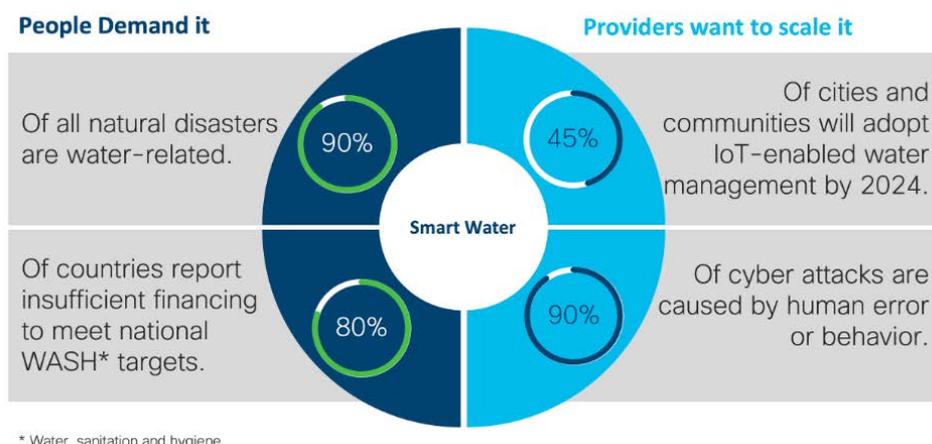


Illustrazione ADL Consulting

Nell'ampio contesto verticale degli impianti di gestione dell'acqua, tradizionalmente perimetro delle multi-*utility*, l'area dei sistemi di controllo distribuiti e quella dell'automazione industriale rappresentano solo alcuni dei principali ambiti tecnologici della trasformazione digitale. L'ambizione finale può quindi riassumersi nel migliorare la supervisione e successivamente nell'introdurre

l'automazione attraverso il controllo retroattivo (*Closed Loop*) degli impianti di trattamento delle acque reflue.

Emergono diversi possibili interventi sulla base degli obiettivi e delle esigenze di contesto che possiamo sintetizzare nell'immagine seguente.



Illustrazione ADL Consulting

L'esperienza progettuale e innovativa portata nell'area degli impianti di trattamento delle acque, ha avuto necessità di considerare lo specifico contesto di intervento, dove:

- le stringenti normative comunitarie in materia di trattamento della qualità delle acque fluviali hanno portato alla necessità, da parte della autorità italiane, di rivedere le politiche di controllo sugli impianti di trattamento delle acque reflue;
- ogni singolo impianto deve essere considerato non più come unità autonoma, ma come parte di un complesso eco-sistema completamente integrato e altamente dinamico;
- il monitoraggio e controllo automatico della qualità delle acque fluviali diventa quindi il requisito di un modello di sistema retroattivo (*Closed loop*) in tempo reale, con caratteristiche predittive e requisiti operativi severi tipici degli impianti del trattamento delle acque

Il risultato dell'introduzione di una progettualità di trasformazione digitale infrastrutturale si identifica nel monitorare e migliorare le prestazionali dell'impianto sia a livello di qualità del processo depurativo che di efficientamento energetico, oltre che a conferire un alto livello di resilienza anche in termini di sicurezza dell'impianto stesso.

La fondamentale definizione in fase preliminare degli indicatori chiave delle *performance* (KPI) del *business* ha consentito un attento e continuo monitoraggio degli obiettivi di progetto e dell'impatto dei sistemi di trattamento delle acque sui citati *business value* (specifici del contesto):

- Qualità dell'effluente – definita come percentuale di tempo del superamento limite da sovraccarichi
- Costi operativi in termini di:
 - Costi energetici (pompaggio, sollevamento, aereazione, trattamento fanghi)
 - Costi per prodotti chimici impiegati nel processo
 - Costo energetico per unità di inquinamento abbattuto per abitante equivalente
 - Costo per smaltimento fanghi
- Sicurezza dell'impianto – direttamente legato e Proporzionale ai valori di MTBF (*Mean time between failures*)

- Effetti riduttivi dell'impatto ambientale
- Miglioramento della qualità complessiva dell'acqua
- Compliance alle normative UE

L'effettiva definizione di KPI legati agli obiettivi appena descritti (*business value*) è rappresentato di fatto da un elenco di parametri oggettivi che rendono effettivamente misurabile l'efficacia e il monitoraggio dei risultati ambiti.

È possibile, di conseguenza, ricondurre a quanto indicato nella seguente tabella (Tab. 1) a puro titolo di esempio di un caso reale, dove sono identificate le 3 principali aree di intervento e i KPI di *business value* associati:

1. Costi operativi
2. Qualità del bene
3. Sicurezza dell'impianto

BUSINESS KPI AREA	CARATTERISTICHE	Unità di misura	Valori attuali		Valori potenziali		possibili % stimate impatto sui KPI
			Min	Max	Min	Max	
COSTI OPERATIVI	Costi Operativi: Costi energetici per abitante equivalente	kWh/AE	18	25	13	16	36%
	Costi Operativi: Costo per prodotti chimici	€/ton. fanghi	30	40	25	30	25%
	Costi Operativi: Costi energetici per inquinante abbattuto	kWh/Kg BOD	2,8	4,5	2	2,3	49%
	Costi Operativi: Costo per smaltimento fanghi	€/ton. fanghi smaltiti	180	260	120	150	42%
QUALITA'	Qualità dell'affluente: Percentuale di superamento limite	%	10	20	4	6	70%
SICUREZZA DELL'IMPIANTO	MTBF	giorni	15	25	30	40	60%
	Sicurezza dell'impianto: Costi per il personale	addetti/1000AE	2	5	0,5	1	80%
	Sicurezza dell'impianto: Costi per manutenzione	% capitale investito	25	30	20	25	17%

Illustrazione ADL Consulting

Il caso d'uso relativo al trattamento delle acque reflue prevede l'obiettivo di predisporre un sistema di supporto operativo per la conduzione dell'impianto di trattamento dei fanghi, mediante innovative metodologie di monitoraggio e controllo di processo, basate su tecnologie digitali abilitanti.

Di fatto, in tale contesto, operare una trasformazione digitale ha comportato primariamente l'inserimento di una corposa presenza di processi di automazione la cui componente di intelligenza decisionale è centrata su utilizzo di modelli matematici basati su sistemi di equazioni differenziali, ordinarie e non lineari, dati dalla cinetica chimica e dai bilanci di massa dei reagenti contenuti nelle acque reflue. Parallelamente la dinamica del bacino idrografico è stata modellata tramite modelli di equazioni differenziali alle derivate parziali della qualità dell'acqua forniti dall'EPA (Agenzia statunitense per la protezione dell'ambiente).

Gli interventi di inserimento degli algoritmi di controllo risultano essere sia di natura *PID Fuzzy*, con *tuning* adattivo basato su modelli predittivi, sia basati su metodologie di rilevamento dei guasti che fanno riferimento a modellazione del dato provenienti da sensori di campo, e relative retroazioni attive sugli attuatori dell'impianto.

Complessivamente gli interventi hanno considerato il riutilizzo, l'ottimizzazione e la messa in sicurezza degli impianti esistenti SCADA, l'inserimento di modelli di comando e controllo retroattivi, a ciclo chiuso, basati su tecniche analitiche e intelligenza artificiale, sostenuti da un'abilitante e resiliente architettura distribuita *Edge2Cloud*, sfruttando le potenzialità dell'*edge/fog computing*, sia infrastrutturale che applicativa.

La soluzione indirizza principalmente le esigenze di digitalizzazione dei processi superando i limiti architetturali esistenti in esercizio, che risultano spesso essere un freno a questo processo di creazione di *knowledge base* e capacità decisionale. Di conseguenza, i principali obiettivi risultano:

- Rimuovere i *silos* applicativi che confinano i dati all'interno delle proprie sorgenti.
- Governare i *dataflow* affinché le applicazioni abbiano accesso ai dati in modo programmato, sincronizzato e puntuale.
- Controllare *privacy*, sicurezza e proprietà dei dati.
- La messa in sicurezza dell'impianto e dell'identità degli oggetti che generano dati/informazioni
- Semplificare il processo di raccolta di dati al fine di identificare informazioni significative e tradurre le informazioni in indicazioni a supporto delle decisioni.

Il valore principale di una architettura *software overlay* per l'automazione di processo è, di conseguenza, il recupero, la movimentazione e la gestione del dato dei dispositivi e dei sistemi di capo, in una forma che sia attendibile, sicura, accurata e temporalmente tracciata, in modo tale da rendere poi disponibile sia ai sistemi e workflow di produzione, che come informazione ad addetti o sistemi esterni.

È altresì importante evidenziare che tale approccio consente l'applicazione del modello indipendentemente dalle eventuali disomogeneità tra linee e diversi ambienti di produzione in termini di sensori e dispositivi di controllo, rendendo possibile comunque l'utilizzo e l'estensione sia in termini di ulteriore automazione di *workflow*, che in altri ambiti operativi, interagendo esclusivamente con i connettori di piattaforma e non con l'intera architettura di controllo di impianto, laddove sia presente.

Il modello nasce quindi per evitare verticalizzazioni applicative per contesto di produzione e per aggiuntive esigenze di automazione dei *workflow*, la gestione di ulteriori sistemi di impianto e il collegamento o correlazione con ulteriori dati eventualmente esistenti.

In conclusione, la piattaforma e il modello implementativo proposto, realizza il *workflow* di gestione dell'operatività di impianto, indirizzando le richieste del perimetro di progetti ma ponendosi allo stesso tempo come *layer* di automazione di processo, i cui principali moduli possono essere richiamati sia per implementazione di successivi processi di automazione che di integrazione ed estensione in altre realtà del gestore degli impianti di trattamento.

Il progetto ha previsto i seguenti risultati:

1. Infrastrutturazione dell'impianto con:
 - i) il *set* minimo di sensoristica indicata che permetta di acquisire in continuo i parametri vitali per descrivere il funzionamento del processo;
 - ii) il *digital-fabric* infrastrutturale di comunicazione e l'applicativo necessario per convogliare ed elaborare i dati raccolti, e implementare le logiche applicative previste al successivo punto.
2. *Operations Support System* che raccomandi e supervisioni l'applicazione delle logiche di controllo manuale dell'impianto nei seguenti *step*:
 - i) periodo di *assessment* delle modalità e delle caratteristiche di funzionamento d'impianto sulla base delle misurazioni in continuo raccolte dalla sensoristica dispiegata;
 - ii) definizione delle logiche di controllo manuale;
 - iii) analisi dell'attuale prestazione dell'impianto, individuazione di eventuali criticità per dare spazio a proposte migliorative;
 - iv) normalizzazione a sistema ed eventuale estensione/revisione delle logiche attuali di controllo manuale dell'impianto, sulla base di evidenze dal *set* di sensori aggiunti all'impianto.

Con le tecnologie abilitanti sopraindicate, si è attuato l'inserimento di 4 categorie architetture quali:

1. Sistemi di misura intesi come sensori/centraline di impianto
2. Infrastruttura in fibra ottica e dispositivi attivi (*switch*) per il collegamento tra sensori/centraline di impianto e il CED
3. Strato applicativo distribuito (FOG) di implementazione delle logiche di misura e analisi e dei dati e controllo di impianto
4. Elementi di infrastruttura centralizzata (cloud/Server) e distribuita (funzioni di *fog computing*) a supporto dello strato applicativo

Il progetto ha consentito la visualizzazione e il controllo dei dati che verranno resi disponibili sia per il monitoraggio dell'andamento di processo e del suo efficientamento che per interventi sull'impianto.

L'impianto in oggetto, per quanto riguarda la linea acque è strutturato come un impianto convenzionale a fanghi attivi consistente oltre ai normali trattamenti primari, in uno stadio di pre-denitro, una successiva ulteriore fase di denitrificazione, seguita poi da uno stadio ossidativo a diffusori sommersi, oltre alla sedimentazione secondaria finale. È presente poi una linea fanghi con digestione anaerobica ed essiccazione.

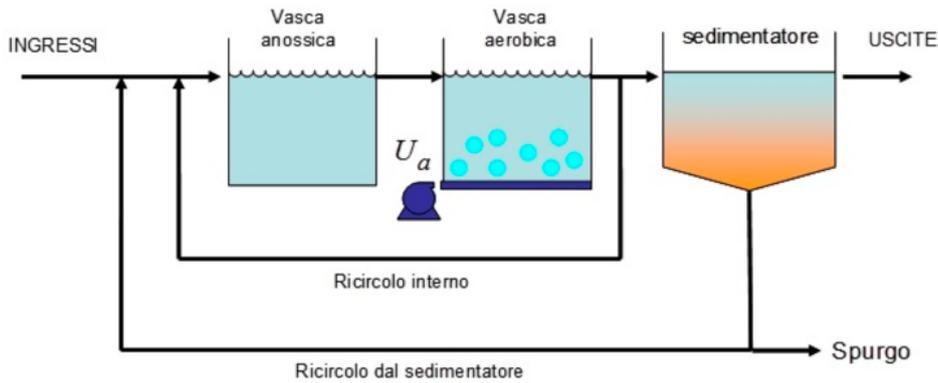


Illustrazione ADL Consulting

L'inserimento delle logiche di controllo e delle tecnologie abilitanti descritte, si cala nel contesto di impianto attraverso uno studio preliminare che ha consentito, già in fase di proposta, di giungere alle seguenti considerazioni:

1. Definizione della famiglia e tipologia dei sensori/centraline di impianto
2. *Retrofitting* di sensori/attuatori esistenti sia in termini di interfacce di comunicazione che applicative definendo connettori standard per la normalizzazione ed "interoperabilità" tra sistemi di diversa natura e fornitore
3. Eliminazione laddove possibile di ogni *lock-in* proprietario
4. Identificazione del percorso all'interno dell'impianto e la stima dei lavori di posa e messa in opera della infrastruttura in fibra ottica e dispositivi attivi (*switch*) nell'area di impianto e locale CED, oltre che connettori verso risorse cloud.
5. Identificazione delle funzionalità di strato applicativo distribuito (FOG) e scelta delle logiche di misura e analisi e dei dati e controllo di impianto
6. Inserimento di elementi di infrastruttura centralizzata (*hybrid cloud/Server*) e distribuita (funzioni di *fog computing* all'interno degli *switch* posti sul percorso della fibra).

La proposta di trasformazione digitale ha assunto caratterizzazioni a fasi all'interno del contesto complessivo di impianto, ove la prima è risultata essere già in linea con un *limited deployment* (evitando così fasi di *pilot* a titolo di pura fattibilità) che insiste solo su un primo impianto, ma che con apposite evoluzioni del modello, ed estensioni, potrà essere replicato in altri impianti, garantendone i principi iniziali e preservando la caratteristica di replicabilità e scalabilità.

È da sottolineare che le caratteristiche scelte per la soluzione proposta considerano un approccio modulare delle 4c componenti tecnologiche abilitanti, che al fine della replicabilità ed estensione consentono genericamente il riutilizzo delle stesse nei seguenti termini:

- Estensione delle funzionalità (ad esempio completa automazione) e ulteriori misure all'interno del sito di impianto (aggiunta di sensori)
 - riutilizzo delle componenti di infrastruttura di fibra e apparati attivi
 - riutilizzo dello strato applicativo locale (FOG) e centralizzato
 - riutilizzo e/o estensione degli elementi di infrastruttura centralizzata
- Replicabilità in altri siti delle medesime funzionalità e misura parte della presente
 - riutilizzo dello strato applicativo locale (FOG) e centralizzato
 - riutilizzo e/o estensione degli elementi di infrastruttura centralizzata

Ulteriore aspetto di notevole valore all'interno del contesto del perimetro di progetto, è stata la definizione delle logiche matematiche che rappresentano un ulteriore vero e proprio *asset* di conoscenza di proprietà della *multiutility* circa le dinamiche di impianto attraverso l'interpretazione e modellizzazione matematica dei dati misurati all'interno dello strato applicativo.

La proposta di progetto ha ottenuto il risultato di predisporre un sistema di supporto operativo per la conduzione dell'impianto mediante innovative metodologie di monitoraggio e controllo di processo basate su tecnologie digitali abilitanti infrastrutturali e applicative.

Per conseguente effetto, si attendono miglioramenti prestazionali dell'impianto sia a livello di qualità del processo depurativo che di efficientamento energetico.

L'aspetto principale da superare inizialmente è generalmente dovuto alla mancanza di dati continuativi sul funzionamento di processo. Questa mancanza è dovuta all'assenza di sensoristica e di un sistema di monitoraggio e supervisione continui sull'impianto, che purtroppo impedisce in fase iniziale la quantificazione dei suddetti miglioramenti prestazionali.

Ad ogni modo, in base all'esperienza e alla conoscenza maturata, si sono individuate le seguenti 4 aree di intervento:

1. Inserimento di un misuratore di portata dei liquami in ingresso
2. Inserimento di un misuratore di ammonio in uscita dalla vasca di ossidazione per misurare il livello di ammonio presente
3. Inserimento di un misuratore di nitriti-nitrati (NOx) in uscita dallo stadio anossico (62C) per valutare il grado di denitrificazione fornito dallo stadio
4. Regolazione della portata del ricircolo interno dalla vasca di ossidazione verso la pre-denitro, riducendo il fenomeno dei solidi sospesi.

L'inserimento della piattaforma ha previsto un approccio di integrazione con le architetture *software* e l'ambiente di impianto di gestione acque in questo modo si è consentita una progressiva e omogenea implementazione dell'automazione di processo ed evitando di insistere su sviluppi *custom* o variazioni onerose dei sistemi di produzione, qualora siano presenti nell'impianto, e nei successivi impianti dell'amministrazione.

La proposta ha contemplato in definitiva una piattaforma di servizi a supporto dei processi di valorizzazione dei dati generati in contesti complessi da sorgenti di varia natura, distribuite in aree vaste ed eterogenee.

In base a quanto descritto fin ora, pur essendo già un esempio tangibile di trasformazione digitale complessa di un sistema di gestione delle acque reflue, ai soli fini di delineare i possibili sviluppi evolutivi del progetto attuale, si possono esprimere 2 possibili funzionalità applicative aggiuntive a valle dei principali interventi:

1. Dotare della necessaria infrastruttura abilitante l'impianto
2. Implementare le logiche matematiche applicative puramente finalizzate alla raccomandazione e supervisione del controllo manuale dell'impianto

Di conseguenza, i successivi sviluppi futuri possono ricondursi alle seguenti aree di azione:

- Affiancamento di un modello matematico simulatore d'impianto che, alimentato dalla sensoristica, ne descriva anche a fini predittivi la dinamica temporale, a supporto dell'effettuazione manuale di decisioni di controllo

- Affiancamento di un modello matematico di simulatore d'impianto e di *soft-closed-loop-controls* che, alimentato dalla sensoristica e simulando le attuazioni, ne descriva anche a fini predittivi la dinamica temporale, a supporto della validazione da parte degli *stakeholder* di impianto di logiche di controllo automatico locali.
- Supervisione e (parziale) controllo automatico dell'impianto sulla base dei *soft-closed-loop-controls*.

BIBLIOGRAFIA



Bibliografia

Indagine conoscitiva sui Big Data

https://www.agcm.it/dotcmsdoc/allegati-news/IC_Big%20data_imp.pdf

Dati e Sistemi Informativi

https://it.wikipedia.org/wiki/Sistema_informativo_aziendale

Electric utility making broadband inroads to unserved, under-served areas

<https://dailyenergyinsider.com/featured/27895-electric-utilities-making-broadband-inroads-to-unserved-under-served-areas/>

Electric Cooperatives, Investor-Owned Utility Form New Pacts to Expand Rural Broadband

<https://www.bbcmag.com/community-broadband/electric-cooperatives-investor-owned-utilities-form-new-pacts-to-expand-rural-broadband>

Nike acquisisce Datalogue

<https://www.sportbusinessmanagement.it/2021/02/nike-ha-acquisito-la-start-up-datalogue.html>

La strategia marketing di Nike - Roberto Serra Blog

<https://www.roberto-serra.com/la-strategia-marketing-lancio-nike/>

Jobs at Nike

<https://jobs.nike.com/it/teams>

GSE

<https://www.gse.it/sostenibilita/storie-e-progetti/economia-comportamentale-e-energia-rinnovabile>

AIops vs Observability vs Monitoring - What Is The Difference? Are You Using The Right One For Your Enterprise?

<https://www.forbes.com/sites/andythurai/2021/02/02/aiops-vs-observability-vs-monitoringwhat-is-the-difference-are-you-using-the-right-one-for-your-enterprise>

Cisco Advances Full-Stack Observability Strategy with Intent to Acquire Epsagon

<https://blogs.cisco.com/news/12082021>

OpenTelemetry: an observability framework for cloud-native software

<https://opentelemetry.io/>

The Rise Of Full Stack Observability And Cisco's Strategy To Fulfill It

<https://www.forbes.com/sites/patrickmoorhead/2021/08/04/the-rise-of-full-stack-observability-and-ciscos-strategy-to-fulfill-it/>

IoT Security Lab: What is IEC62443

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/IoT_Security_Lab/IEC62443_WP.html?dtid=oblgcdc000651

Securing industrial networks: What is ISA/IEC 62443?

<https://blogs.cisco.com/security/securing-industrial-networks-what-is-isa-iec-62443>

Security & Trust: i motori dell'innovazione nella trasformazione digitale

<https://gblogs.cisco.com/it/2020/03/03/security-trust-i-motori-dellinnovazione-nella-trasformazione-digitale/>

NIST Best Practices in Cyber Supply Chain Risk Management

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cyber-supply-chain-risk-management.pdf

Italia Digitale 2026

<https://innovazione.gov.it/dipartimento/focus/italia-digitale-2026/>

Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities

https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf

Legge 4 agosto 2021, n. 109. Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

<https://www.gazzettaufficiale.it/eli/gu/2021/08/04/185/sg/pdf>

Linee guida per l'adattamento ai cambiamenti climatici della città di Milano

https://partecipazione.comune.milano.it/uploads/decidim/attachment/file/325/Sub_allegato_5_DEF_Linee_Guida_PAC_.pdf

Orange Book 2018

<https://www.utilitatis.org/my-product/orange-book-2018/>

Orange Book 2017

<https://www.utilitatis.org/my-product/orange-book/>

Orange Book 2015

<https://www.utilitatis.org/my-product/orange-book-2015/>

