

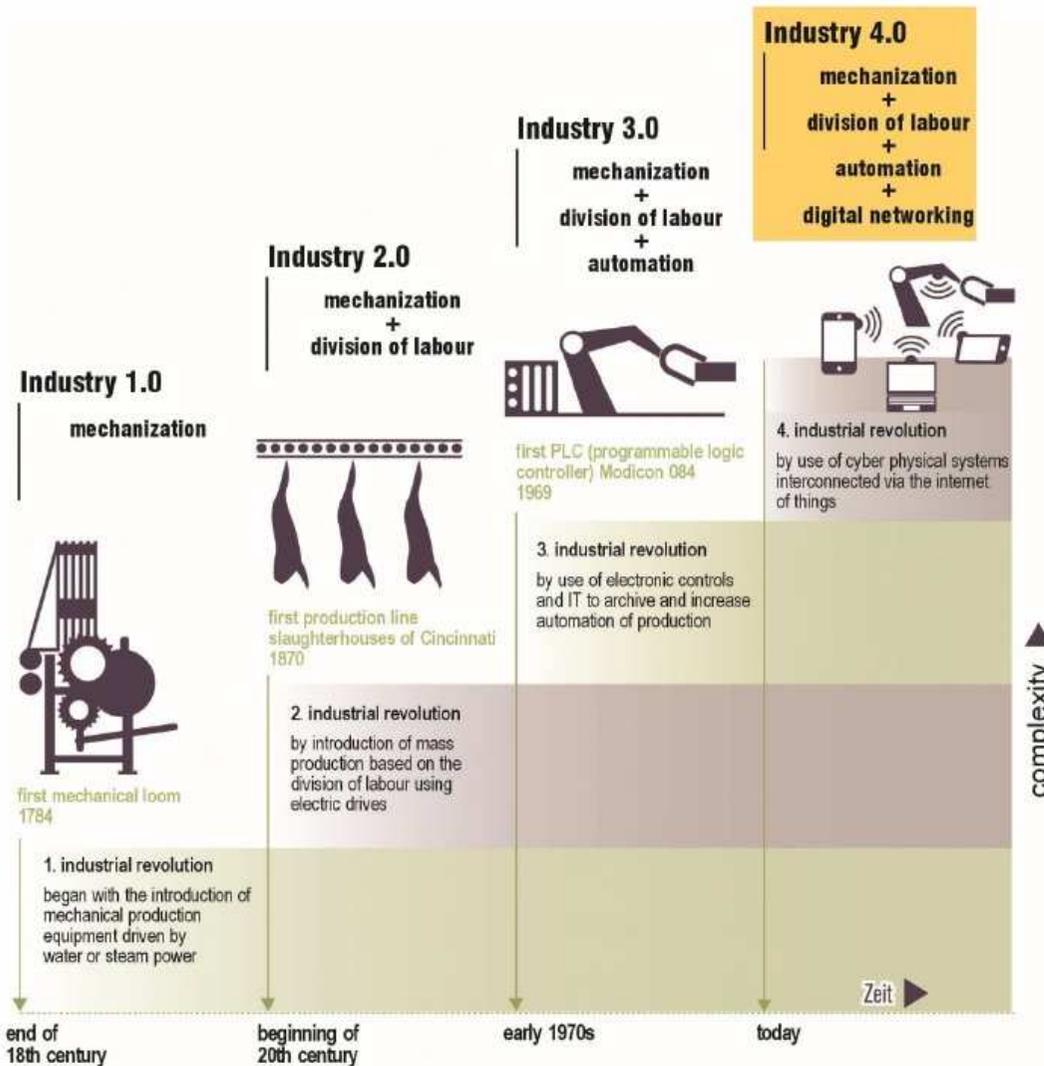


Raccolta e sintesi delle informazioni in Sicurezza

Supervisione multi-impianto
Assistenza da remoto
Cyber Security

Quart (AO), 20 Settembre 2019

C. Brocca, D. Barban



industrializzazione

il lavoro umano viene supportato da sistemi meccanici (macchine a vapore)

ottimizzazione

il lavoro umano viene supportato da sistemi elettromeccanici (macchine elettriche)

automazione

aumento della produttività grazie a linee di produzione automatizzate

digitalizzazione

integrazione tra IT (information technology) e processo produttivo

Fonte: DFKI, Implementation recommendations for the future project Industry 4.0 (Research Union / Acatech, 2013)

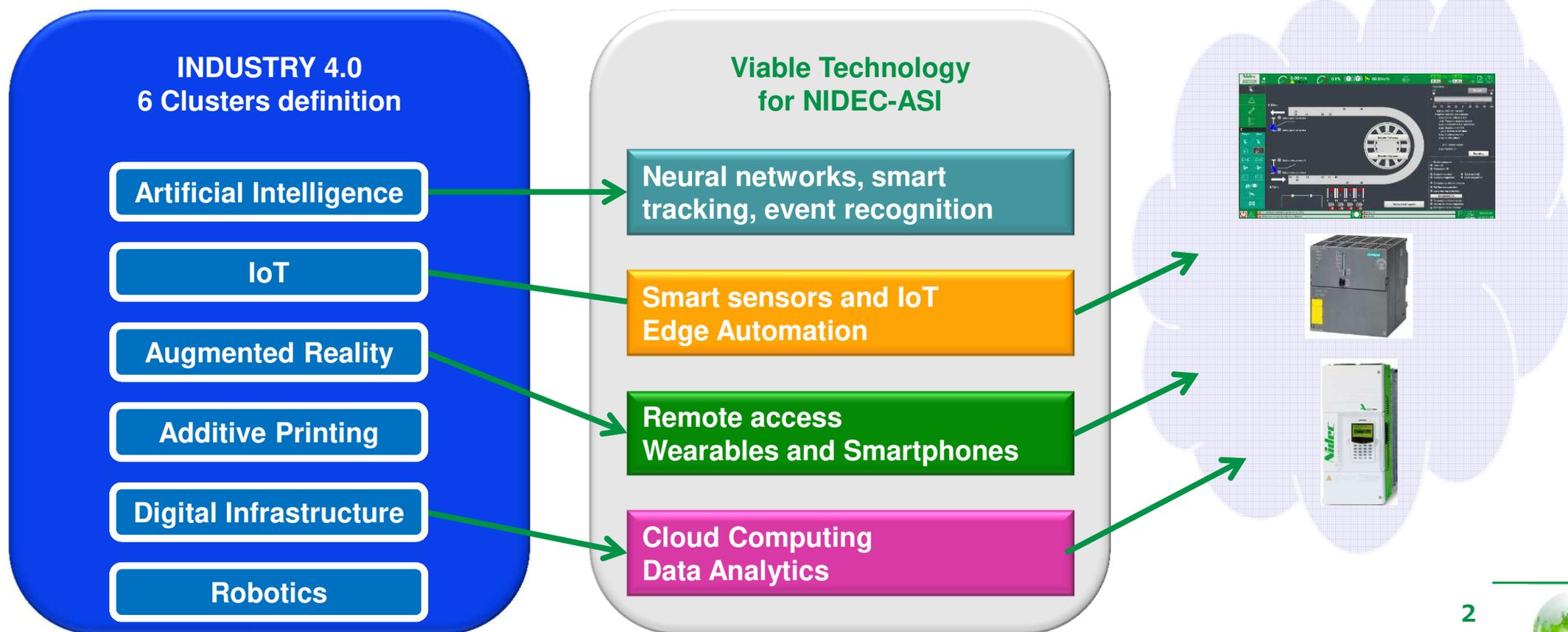


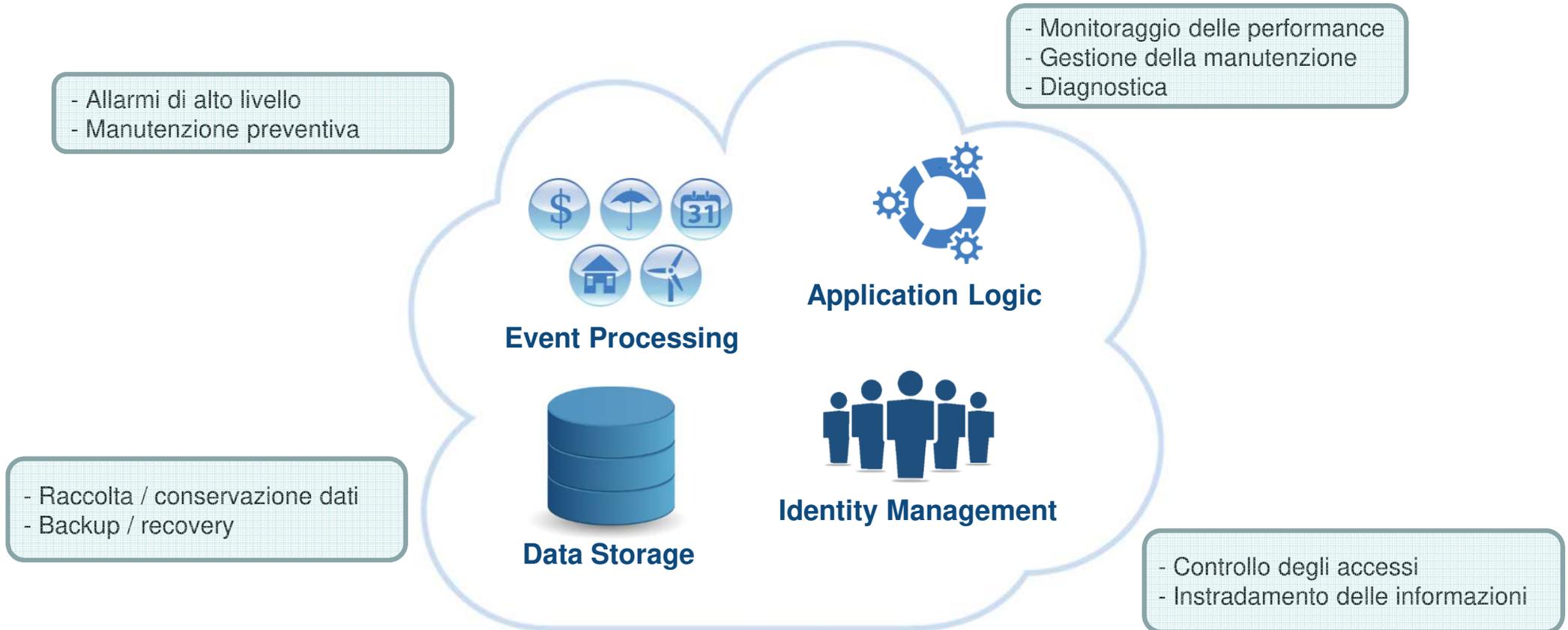
Clusters di Industria 4.0

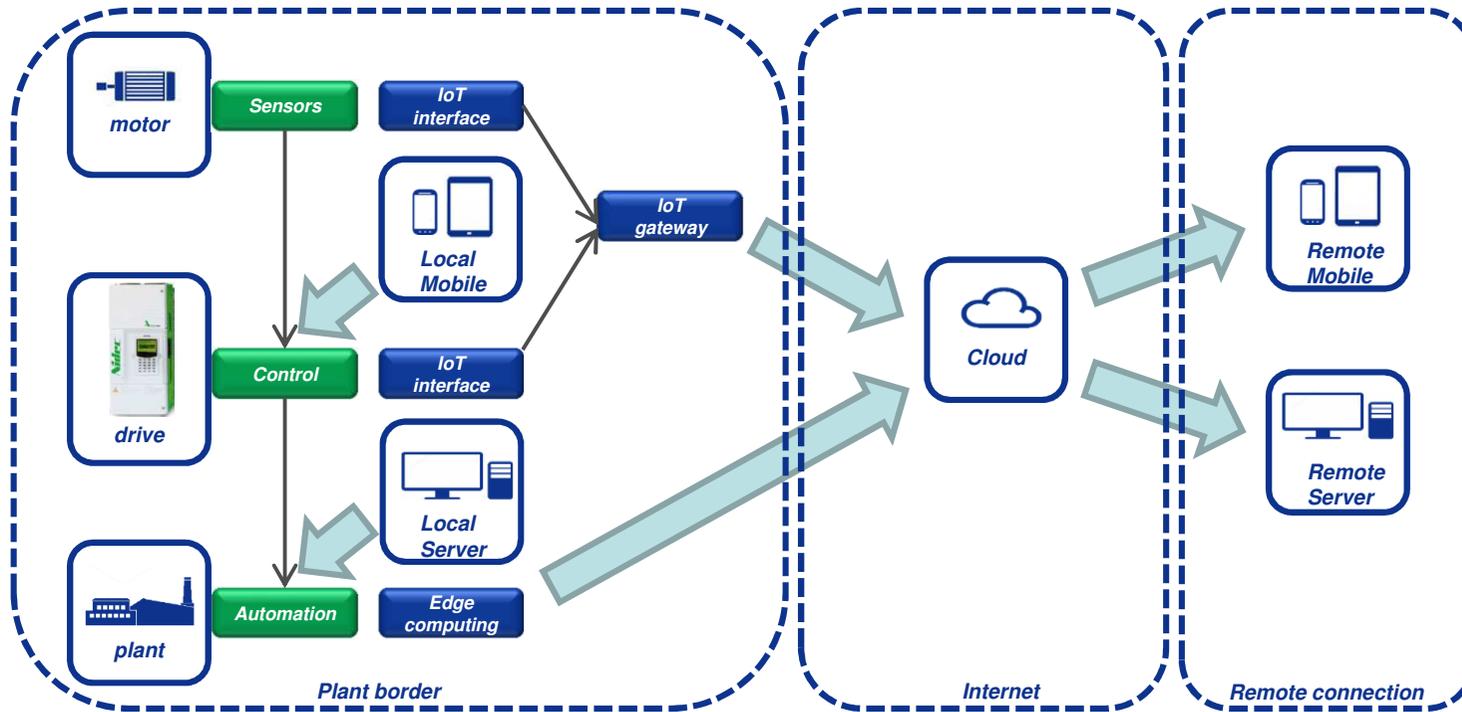
La digitalizzazione sta cambiando l'industria e la società su vasta scala.

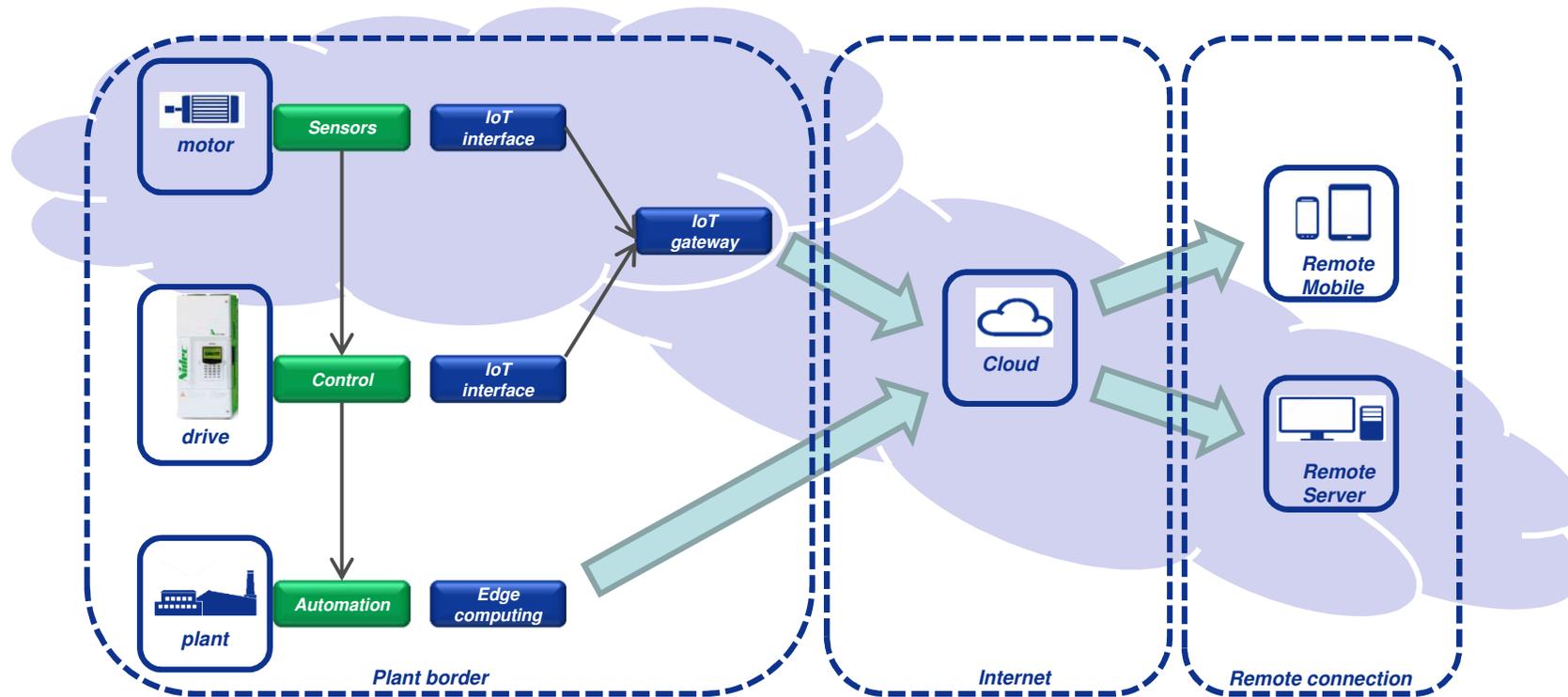
Ogni settore industriale è coinvolto in una qualche forma di trasformazione digitale, sia spostandosi nel cloud, imprigionando l'analisi dei big data per ottenere informazioni e previsioni vantaggiose in ambito aziendale, sia implementando una qualche forma di Internet of Things.

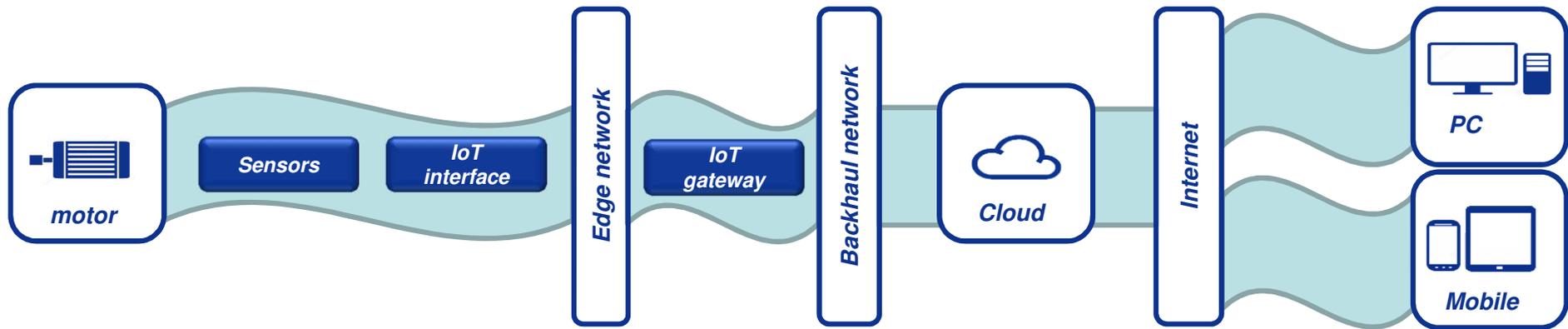
In un ambiente cloud, le risorse e le applicazioni informatiche vengono fornite come servizi su una rete, in genere Internet.

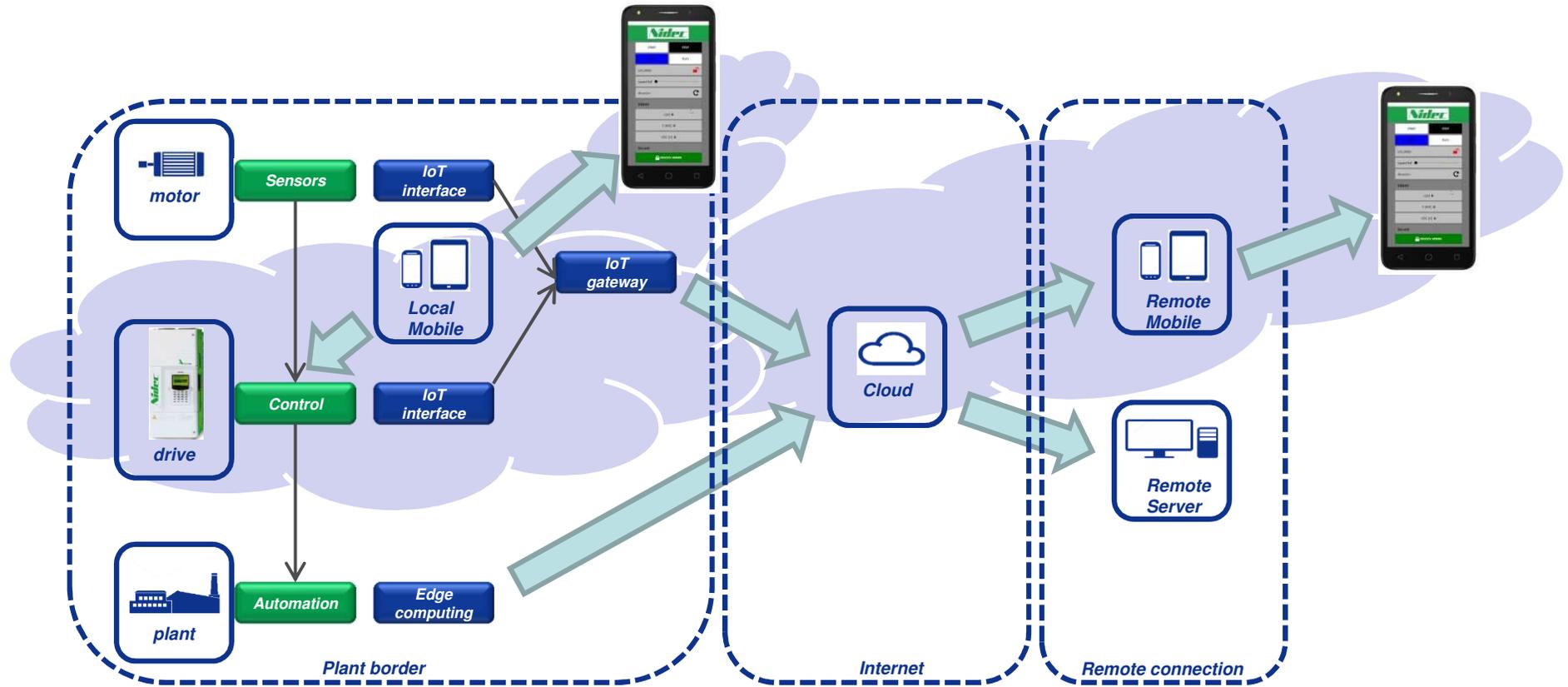










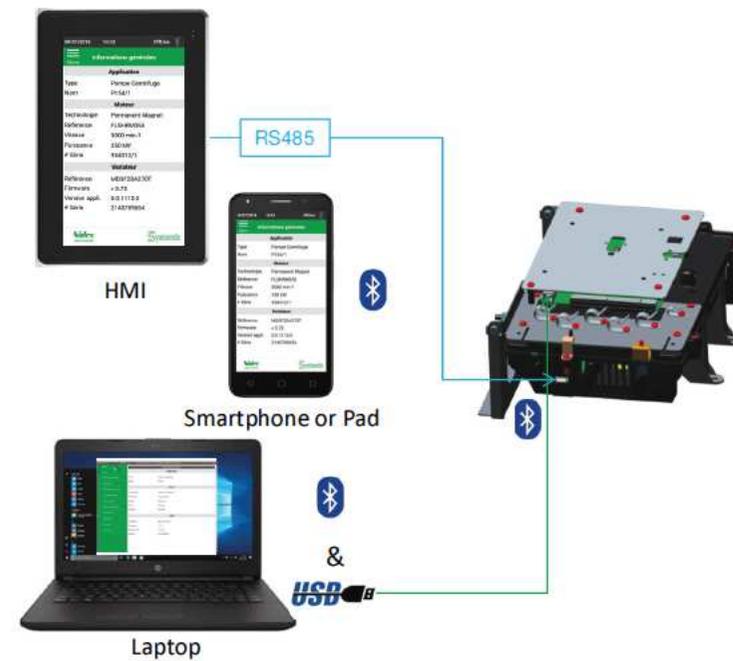




Connessione locale
Accesso ai parametri



Backup parametri



Collegamento Bluetooth

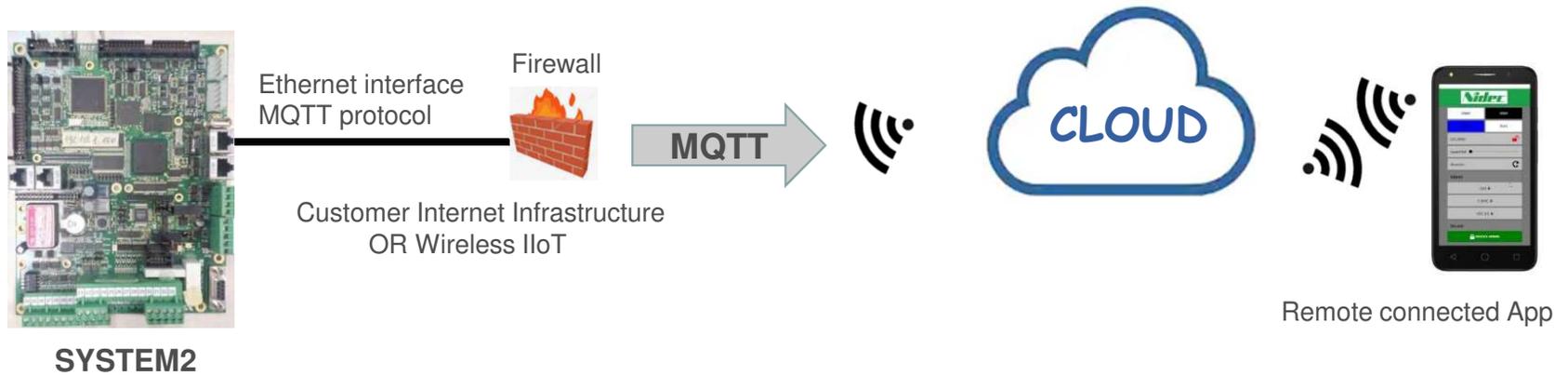


DVM APP – collegamento locale / remoto

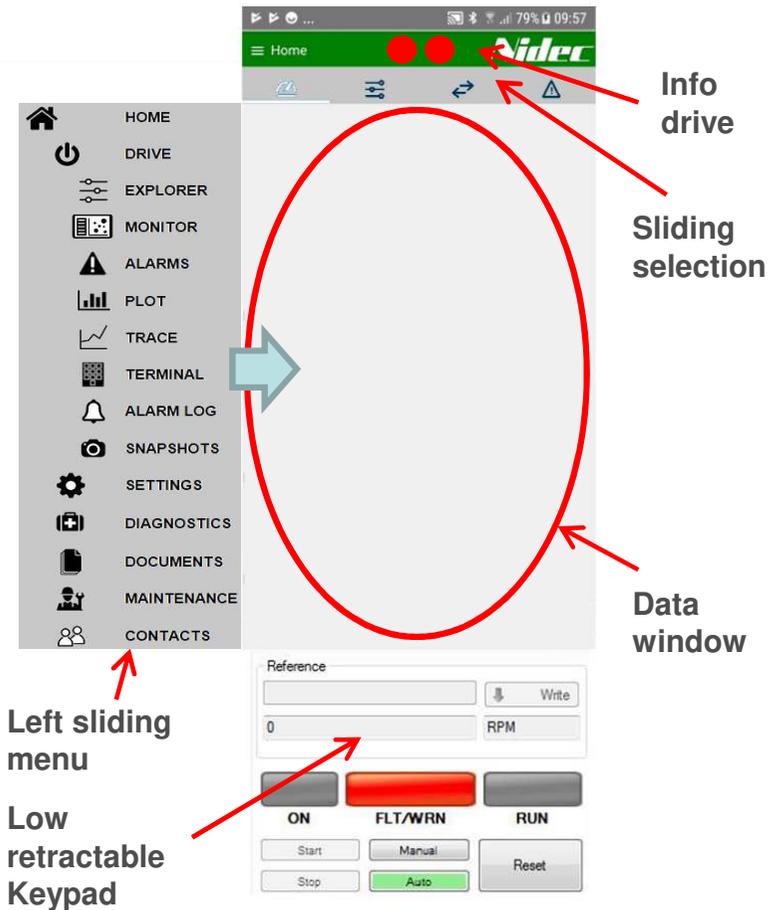
1st step



2nd step



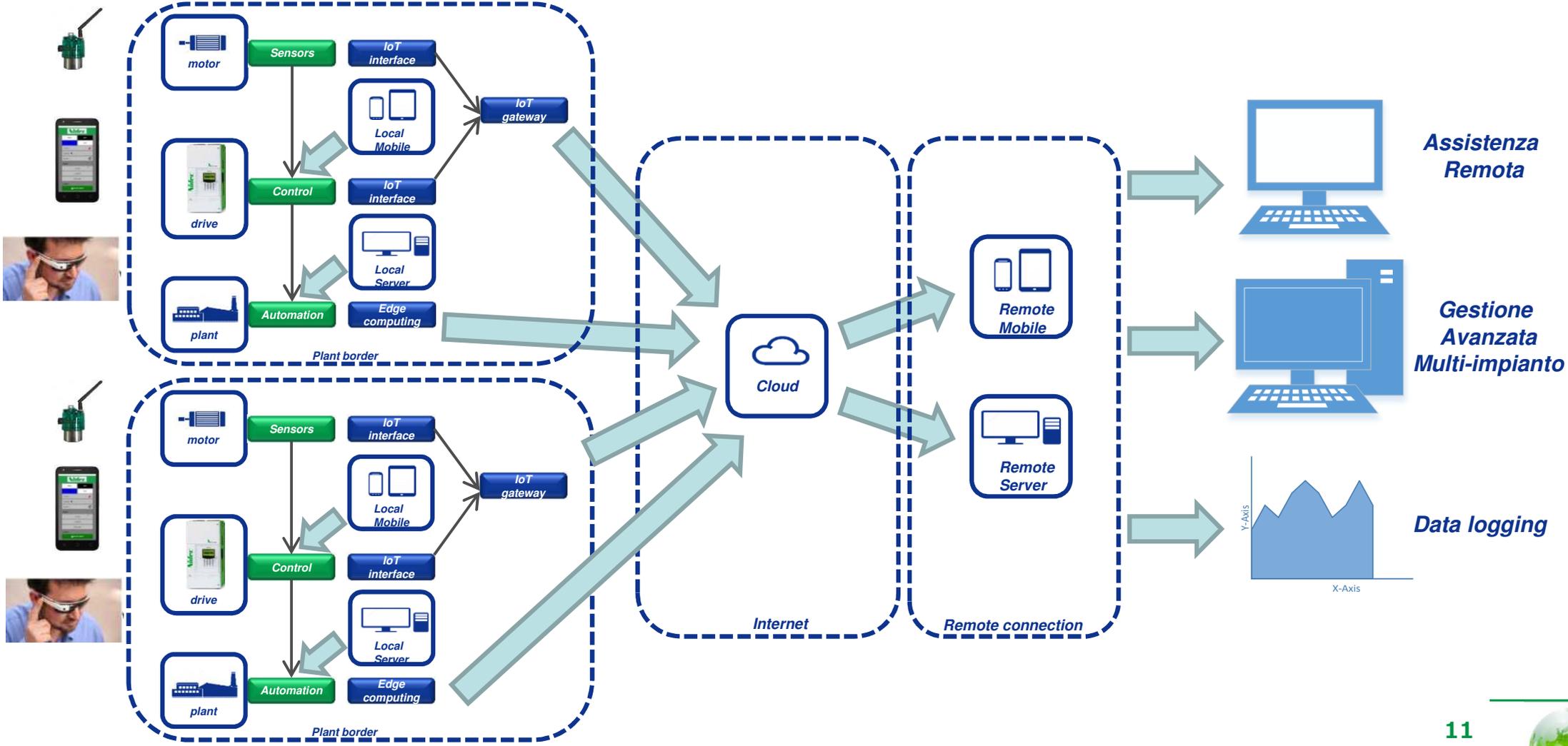
DVM APP - funzionalità



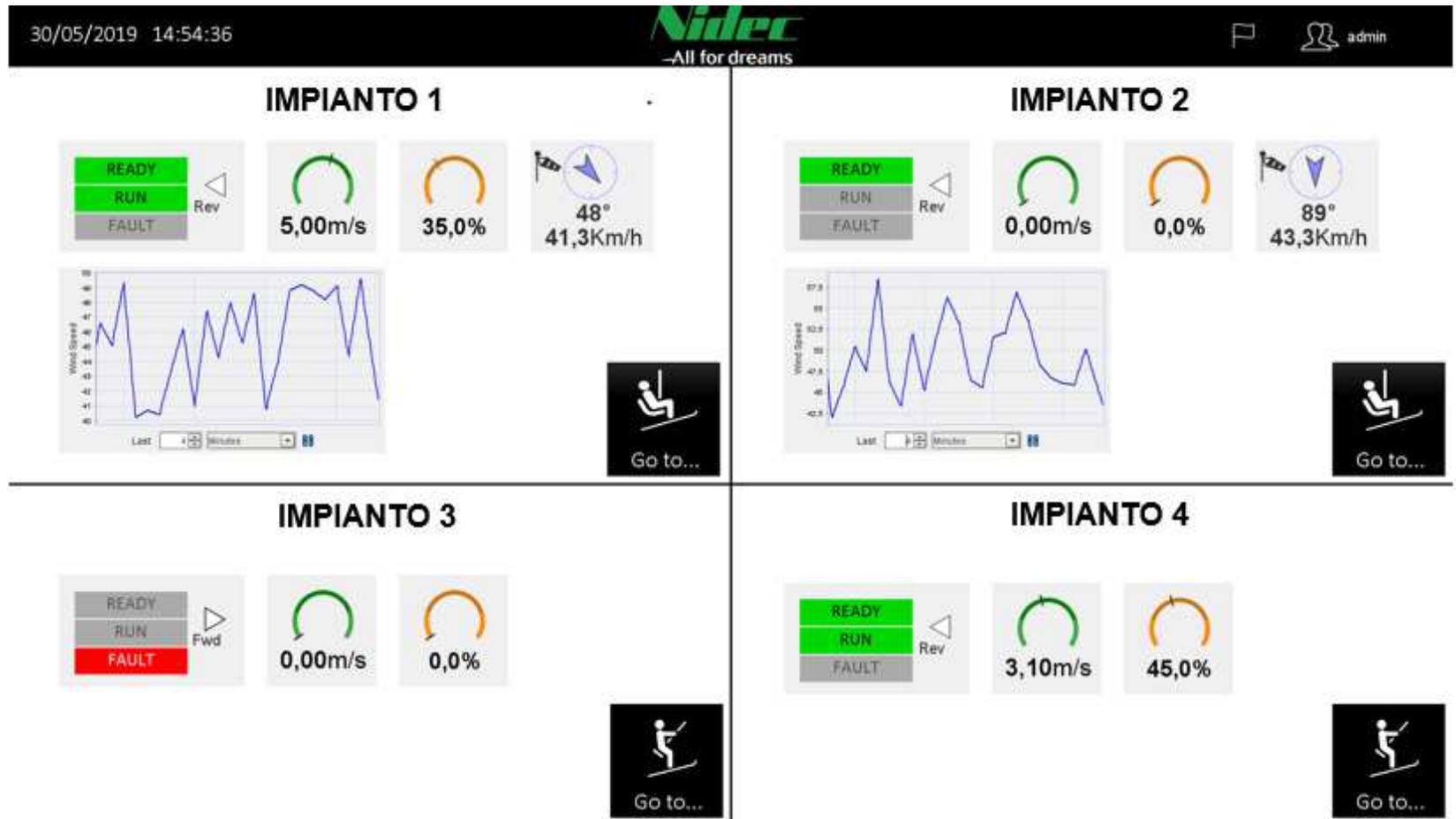
DVM APP drive configuration, maintenance e service features

- **DRIVE CONFIGURATION**
 - Explorer, Monitor, Alarms, Plot, Trace, Terminal, Alarm Log, Snapshots
- **MAINTENANCE FEATURES**
 - Diario di Manutenzione (Attività pianificate, attività eseguite ed archivio)
 - Gestione delle Attività (prossima attività pianificata, descrizione delle attività, associazione attività-drive)
 - Procedure (descrizione attività di manutenzione, spare parts, analisi dei guasti)
- **SERVICE FEATURES**
 - Gestione documentazione di impianto (Manuali, Unifilari, Schemi funzionali), repository locale (drive o local server) e remoto (cloud o NIDEC website)
 - richiesta di intervento remoto ed attivazione telecamera dello smartphone per funzioni di remote monitoring

Servizi da remoto



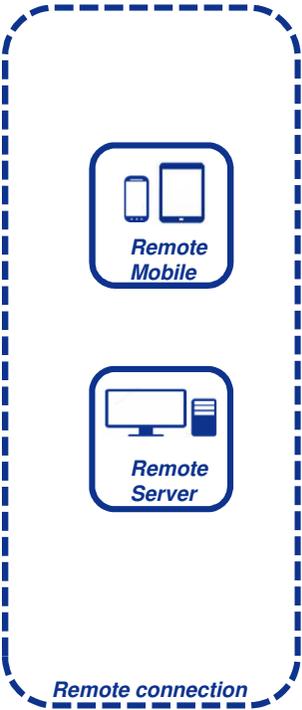
Gestione avanzata multi-impianto



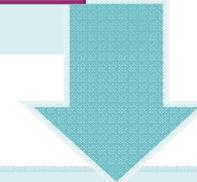
Remote connection



Data-logging (IBA)



NUOVE TECNOLOGIE



NUOVE TECNOLOGIE per VECCHI PROBLEMI



Cosa può andare storto

Da: [REDACTED]

Inviato: domenica 25 novembre 2018 20:33

A: [REDACTED]; [REDACTED]

Oggetto: Virus attack Vorobievi gory installation

Hello dear colleagues, I need to inform you that today morning our installation was attack by unknown virus which encrypts all files in PLC. We took PLC from bottom station and installed it to driving station , but it was not modified that why installation running but with errors. Maxim was trying to fix the PLC with antivirus but unfortunately it didn't work. Tomorrow morning before opening we have to make conference call and make decision.

We will come to installation 8.00 o'clock and will waiting for your instructions.

Regards [REDACTED]

Moscow's First Cable Car Shuts Down After Opening in Suspected Cyberattack

Nov. 29, 2018



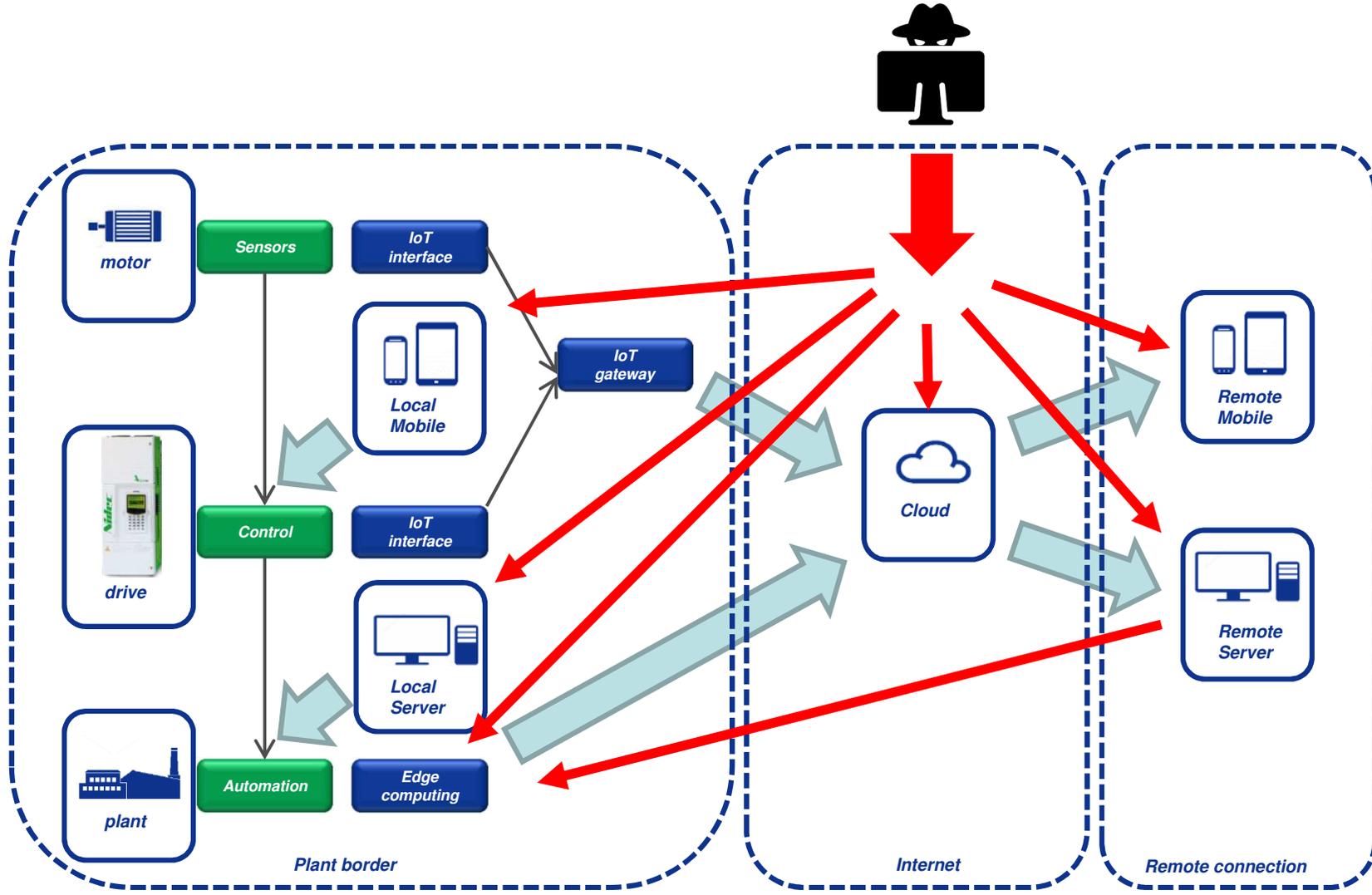
MUST READ: [The irrelevant iPhone 11: Apple will crush Android with services, bundling, and cheap devices](#)

Moscow's new cable car system infected with ransomware two days after launch

Cable car system is now back up and running after a two-day downtime.



Digitalizzazione → I Sistemi di Controllo sono raggiungibili dall'esterno





Riservatezza: l'informazione non è resa disponibile o divulgata a persone, entità, processi non autorizzati

Integrità: l'informazione è protetta da modifiche o distruzione

Disponibilità: l'informazione è accessibile ed utilizzabile su richiesta delle persone, entità, processi autorizzati



	Machinery Safety	IT-Security
Obiettivi	Prevenzione degli infortuni/incidenti	Riservatezza, integrità disponibilità
Dinamica	Settore abbastanza statico (uso previsto, contromisure prevedibili)	Settore altamente dinamico (manipolazione intenzionale, intento criminale)
Misure per la riduzione (mitigazione) del rischio	Principalmente dal costruttore in uno specifico momento (fornitura della macchina)	Da vari attori (costruttore, system integrator, utilizzatore, service provider) in modo continuativo per tutta la vita della macchina



Security e Safety sono legate nell'ambito delle macchine

I Sistemi di Controllo sono raggiungibili dall'esterno



I Sistemi di Controllo sono attaccabili dall'esterno. Possibilità di:

Accesso a informazioni riservate

Perdite economiche

Danni ai macchinari e/o alle infrastrutture

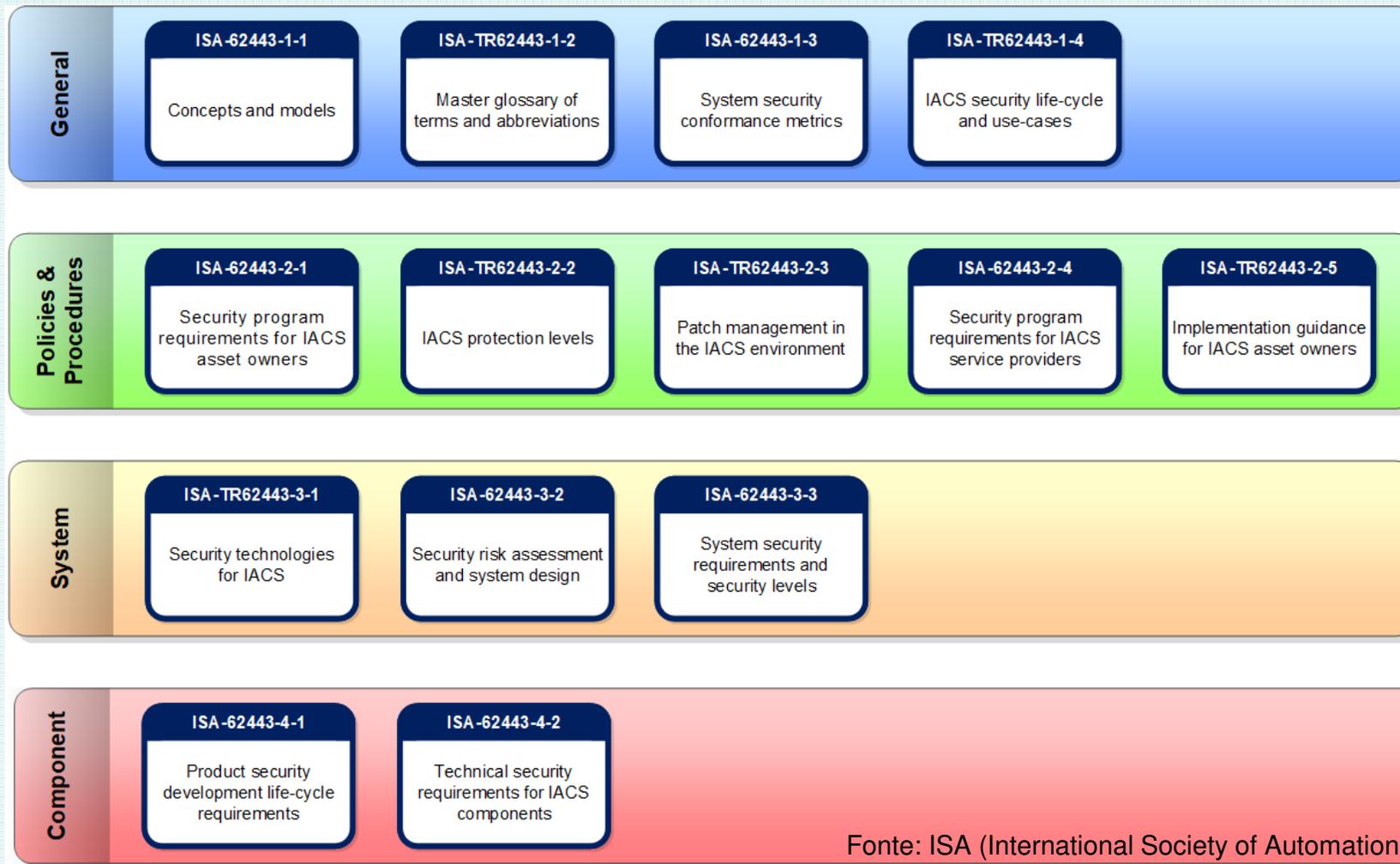
Danni alle persone

Nell'ambito dell'automazione industriale l'integrazione tra Information Technology e Sistemi di Controllo comporta che la Sicurezza Informatica abbia rilevanza anche sulla Sicurezza delle Persone!



Come ci si difende: alcuni riferimenti normativi

• ISA/IEC 62443 Standards



Fonte: ISA (International Society of Automation)



Come ci si difende: alcuni riferimenti normativi

- **ISO/TR 22100-4:2018**

Safety of machinery - Relationship with ISO 12100

Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

This document gives machine manufacturers guidance on potential security aspects in relation to safety of machinery when putting a machine into service or placing on the market for the first time. It provides essential information to identify and address IT-security threats which can influence safety of machinery. This document gives guidance but does not provide detailed specifications on how to address IT-security aspects which can influence safety of machinery.

This document does not address the bypass or defeat of risk reduction measures through physical manipulation.

- **IEC TR 63074:2019**

Safety of machinery - Security aspects related to functional safety of safety-related control systems

...gives guidance on the use of IEC 62443 (all parts) related to those aspects of security threats and vulnerabilities that could influence functional safety implemented and realized by safety-related control systems (SCS) and could lead to the loss of the ability to maintain safe operation of a machine.

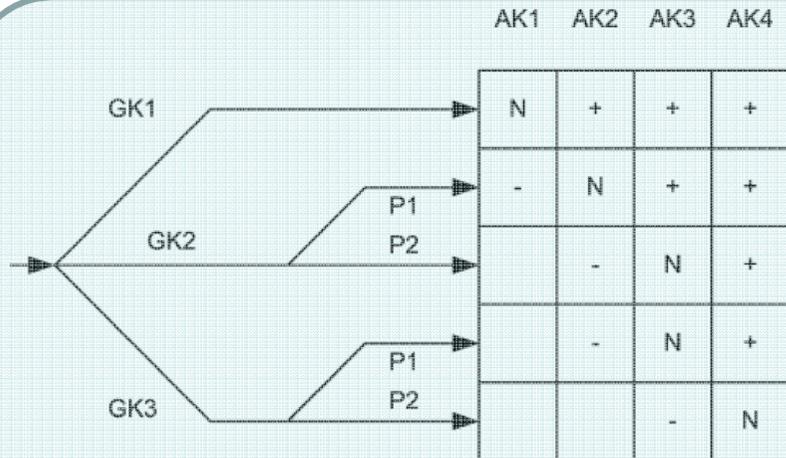


Safety risk - Security Risk



Classificazione del rischio

AK → Requirement class (EN 13243)



Parametro	Descrizione
GK	Livello del pericolo
P	Possibilità di evitare il pericolo

SL → Security level (IEC 62443-3-2)

Security Level	Descrizione
SL 1	Protezione contro violazioni casuali
SL 2	Protezione contro violazioni intenzionali che impiegano mezzi semplici, con poche risorse, competenze generiche e bassa motivazione
SL 3	Protezione contro violazioni intenzionali che impiegano mezzi sofisticati con risorse moderate, specifiche competenze IACS e moderata motivazione
SL 4	Protezione contro violazioni intenzionali che impiegano mezzi sofisticati con ampie risorse specifiche competenze IACS e alta motivazione



Sicurezza: cinque passi essenziali

Identificare

Identificare le minacce e le vulnerabilità del sistema: Perché posso essere attaccato ? Cosa ho di importante ? Quali sono le mie vulnerabilità (interfacce) ? Che risorse sono fondamentali per le funzioni critiche del mio impianto ?

Proteggere

Sviluppare e implementare le appropriate misure di protezione per prevenire o limitare l'impatto di un attacco (es. By design, controllo accessi, formazione,...)

Individuare

Sviluppare e implementare le appropriate misure di per identificare un attacco in corso (monitoraggio eventi / anomalie /processi)

Rispondere

Sviluppare e implementare le appropriate attività per fronteggiare un attacco, in modo da fermarlo e limitarne gli effetti (es. pianificazione)

Ripristinare

Sviluppare e implementare le appropriate attività per ripristinare quanto è stato compromesso da un attacco in modo da ridurre l'impatto dell'attacco.



Videa

— All for dreams